

# Mao Declaration

## Exhibit 1

Redacted Version of Document  
Sought to Be Sealed

GOOG-BRWN-00406065

## Message

**From:** Lorraine Twohill [lorraine@google.com]  
**Sent:** 1/29/2021 3:30:31 AM  
**To:** Sundar Pichai [sundar@google.com]; Rahul Roy-Chowdhury [rahulrc@google.com]; Jen Fitzpatrick [jen@google.com]; Luiz André Barroso [luiz@google.com]  
**Subject:** Today is Data Privacy day...so please read!

Hi folks,

As today is International Data Privacy Day (check out our [homepage](#)), and Privacy has been on my mind, as well as all of yours for some time, I wanted to share some thoughts. It has been almost 11 years since I first spoke at Exec Circle (and Ben listened!) about User Trust and needing a Google Account with controls. And 7 years since I did the User Trust tgif. I have been doing a lot of thinking (and asking!) over the years. And we have made a lot of progress but our challenges are even greater. We need more velocity! So, since I know you all agree, and I know Sundar that you have been thinking about this too, I wanted to share my random thoughts here, as hopefully somewhat useful and actionable. And yes there will be reasons why a lot of this is hard, but we are at our best when solving really hard problems! And then just maybe we could get to this vision that we put together just over a year ago,

With the greatest of respect, and apologies in advance for my ramblings...

L.

What I think we need:

- 1.
2. Much more visible comms on and off product
- 3.
- 4.
5. Privacy as a feature/products making meaningful change
- 6.
- 7.
8. Definitive progress in ads, including showing that we are ok losing out too
- 9.
- 10.
11. Owning our absolute strength in security
- 12.
- 13.
14. Other random ideas that could help

#### 1. Much more visible comms on and off product

In 2020, we sent over [REDACTED] users to our privacy check ups and [REDACTED] to our security check up from our homepage and promo efforts. But it feels completely separate from those *moments of truth* when a user is in-product and needs our help. What if we:

- 
- **Roll-out a consistent 'Safer with Google' brand system and icon more aggressively across our products.** There's a number of moments in product where we already use the shield and messaging to signal

privacy and security protections (e.g., "only you can see this" for Google Account related queries in Search and in My Activity). But we need to accelerate implementation across PAs so it shows up in the products people use every day.

- 
- 
- **Increase user facing reassurances in-product:** No more unexplained features or cross-product data usage that freaks a user out. We know that a feature can trigger user concern over how their data is being used and why (particularly x-app). Increase investment and prioritize [REDACTED] to provide users with helpful transparency, education, and access to their controls in these moments.
- 
- 
- **Explain ourselves much, much better. And do that everywhere.** This is not new work but is a compelling way of talking about the data we have, 3 types of data, stuff you save, stuff you do (your activities) and stuff we use for ads (much smaller). If we did this well, everywhere, including in your Google Account, it would help a lot.
- 
- 
- **Move our promo real estate to the TOP of the screen in mobile.** Instead of push-up promos, move them to the top of the screen so they are unmissable. Instagram P&S promos are at the top of the screen, Twitter's promos are overlays. At the bottom of the screen, ours don't have the same gravity and visibility, making our P&S messages feel unimportant/optional. By adding some friction we will increase engagement and demonstrate to users and KOFs that privacy and security are a top priority.
- 
- **Establish GSEC(Google Safety Engineering Center) in the US.** Building on the successful launch of GSEC Munich (and GSEC Dublin) let's identify key offices where we have strong privacy efforts (e.g. Cambridge for Chrome) and establish GSEC in the US as a key part of our KOF outreach efforts.

## 2. Privacy as a feature/products making meaningful change

We need more products built upon our privacy north star that PDPO has been championing. Our collaboration with Pay is a good example of how a product can build privacy and security right into the product ('A safer way to pay'). But there is more that is needed to ensure that across the company we live up to the new privacy principles and develop consistent, scalable privacy features that bring those principles to life. Could we start with:

### Giving users more transparency and control over their data

- 
- **Apps have to ask permission to access your data,** not just assume that all of Google can access. By asking users permission to link their Inbox with Maps, we can avoid trigger moments like hotel reservations showing up in Maps. Or at least we show a card the first time it happens, to explain that App A knows this info from App B. (Vault could be a great answer here)
- 
- 
- **All products to be transparent on data usage.** What is tracked, what is it for, what is in it for the user; give users ability to turn off ANY of the data in any of the products in a way that they want. Introduce 100% comprehensive and consistent data use labeling: anytime and everywhere we use user data.
- 
- **Make it easier for users to delete data.** Streamline the current path - go to Google Account, Click on Data & Personalization, Click on My Activity, Click on Delete and go from there - by further improving the delete actions in Google Account and surfacing 'delete activity' in key product surfaces. Make delete feel easy



and immediate. Let's more aggressively surface 'auto delete' options and make it easier for people to access the tool

- 
- 
- **Give users the option to choose from pre-packaged settings bundles (low, medium, high).** Based on "user profiles" (e.g. recommend to set data retention to 3 months, actionable in a simple one-click way: you choose the "type" you want (e.g. full anonymity, balanced setting, enable all data sharing), and this applies automatically across all Google settings. Like the "privacy slider" idea we had years ago.
- 
- 
- **Continue to improve Google Account as the single destination for users' privacy and security choices.** Elevate controls more visibly to account homepage, add new products and features, like our password protection (e.g. Build "LifeLock" into the Google Account. People pay for services like LifeLock to protect them from identity theft - a constant concern and growing with more online commerce. Could make it an G1 upgrade feature.

#### Creating more visible, ownable privacy products and brands:

- 
- **Vault/keeping my most important documents 'off the grid', like a private cloud for (sensitive health info, taxes, property deeds, passport, etc).** The Vault idea has been knocking for many years now, a clear product opportunity exists to give people ultimate control and keep their most valuable digital stuff safe.
- 
- 
- **Make Incognito mode truly private:** Make Incognito mode truly private [REDACTED]  
[REDACTED] We are limited in how strongly we can market Incognito because it's not truly private, thus requiring really fuzzy, hedging language that is almost more damaging

#### 3. Make faster and more demonstrable progress on ads

Users point to our ads as THE reason why they can't trust Google and why they think we sell their personal information to 3rd parties. While we have made great progress with things like our recent Privacy Sandbox announcement there is more we need to do here faster. We could start with:

- 
- **Focus on where we think the long term is in Ads.** Be more focused about which parts of the ads business we want to get behind (i.e. real time bidding on user data = bad; contextual ads in search = good). With [REDACTED], we will be taking a more declarative stand on what we think are acceptable uses of data on the web. It will allow us to distance ourselves from cross-site tracking while reiterating the importance of direct relationships between people and the brands/publishers they choose. However, [REDACTED] is scoped to just the web - we need to accelerate efforts to align on a consistent set of practices across all the places where people see digital advertising, including mobile (Android, iOS), and connected TV.
- 
- 
- **Improve Ads Settings/make this a much bigger deal:** Let people see what is used to target them and let them adapt it/change it/suggest new things. This [page](#) is decent, we need to tell people about it in product and link to it, and we need to promote it and also make it better.
- 
-



- **Making Mute this Ad a more valuable property.** Every ad has 'mute this ad' but the current experience is limited and does not allow us to tell our story to our users. Can we add more transparency about why they're seeing this ad, point to ads settings controls, more opportunities to engage users, more space to tell our story to make this a more valuable experience for our users.
- 
- 
- **Accelerating potential changes in ad retargeting.** This is one of the top triggers for users when it comes to concerns that Google tracks them and shares/sells their information with 3rd parties. Explore options ranging from making it easier for people to opt-out in the moment (e.g. 'stop personalized ads for me' button), to changing timing of retargeting (e.g. increase time lapse) or specificity (e.g. less specific). Accelerate efforts underway within Ads to address this and improve the consumer experience:
- 
- 
- 
- **Further accelerate Privacy Sandbox efforts:** As part of the Privacy Sandbox effort to replace 3P cookies in Chrome, there are technology proposals to enable brands to deliver tailored ads to those who have had prior interaction with their site (i.e. retargeting) - but in a way that would not be as specific to an individual product (e.g. ad for men's running shoes vs. ad for Size 12 Men's Blue Nike Cross-Trainers)
- 
- 
- **Push for Privacy Norms faster:** In parallel to Privacy Sandbox, Ads is working to get internal alignment on a set of privacy norms / commitments that would govern how Google's ads products work. There are norms being discussed that would impact retargeting in areas such as timeliness (ensuring there is some delay before retargeting ads appear to avoid 'spooking' users with their immediacy); ensuring that there is a time cap on how long retargeting ads appear to avoid annoying users); frequency (ensuring there is a limit on # of times retargeting ads are shown); specificity (ensuring that the information surfaced in the ad is relevant but not overly specific such that it causes concern).
- 
- 
- **Increase velocity around Experiments:** Beyond the Privacy Sandbox and Privacy Norms efforts, there are also user experiments being conducted in Ads, such as one that notifies users at the point that a website is attempting to add them to a retargeting list, giving them an option to opt-out
- 
- 
- **Explore tagging ads that preserve privacy.** Introduce a visual system for Ads that (in the future) are served in a privacy preserving way (i.e. targeting via Privacy Sandbox technology, handled on device, anonymized). Make this work across all surfaces, building from Chrome. Brand these ads!
- 
- 
- **Mythbust Data Selling:** ■■■ of users believe we sell their data. We need to do more to communicate to them **in-product** that their data is never sold and never shared without their permission.

#### 4. Owning our absolute strength in security

We do a lot to keep people safe across Chrome, Android, Gmail and your Google account but people have no idea. We keep lots of KOFs safe and governments, but do we tell them? Users see privacy and security as two sides of the same coin so our leadership here is a huge opportunity. Could we:

- 
- **Develop a bolder Security claim.** What is the equivalent of "Never sell our users' personal information to anyone" for Security. Our current version ("Build the strongest security technologies into our products") does

not seem bold enough. Can we own Safest? Back up with reasons to believe like [REDACTED], [REDACTED]

[REDACTED], [REDACTED].

- 
- 
- **Humanize our Security efforts:** The Defend the User project: tell the stories of the people behind the security features. We have some of the world's top minds working on our security technology - let's tell that story. Have our security engineers interact with DC and local govts more too.

- 
- 
- **Add helpful security tips to every security email.** The emails we send to verify when users have signed into a new device are the most frequent email we send - super high volume and frequency of impressions - so much so that there are memes online about Google Security detecting anything suspicious

- 
- 
- **More visibly surface security benefits in user comms.** Remind users of all the occasions where we have their back. One of the reasons MSFT is scoring well on security is that you have to consciously update versions, install virus protections, etc. In our case we do a lot of that invisibly (in Chrome/Chrome OS/Android/Play Protect/Gmail). For example we could: send a monthly Safety summary (x many emails we put into spam for you, x many websites we have flagged as dangerous, security features of our latest Chrome/Android release), we could provide similar info and further safety tips on a "new tab" each time you open one, etc.

- 
- 
- **Treat users like VIPs when security issues arise:** Beyond communicating how we're activating our 'automatic' protections, such as spam protections in Gmail, we can provide detailed (yet simple!) reports to users when we've addressed a more significant issue such as an Account hack. For more significant security issues, let's connect users with a real person (or at least help make our automated help feel as personalized as possible). Provide reassurance to users, and extend the opportunity for additional dialogue / more information if they have further questions or concerns.

- 
- 
- **Incentivize users to use our security features.** Put our money where our mouth is. Show that we care about our users' safety so much we will reward them for turning on 2sv, using Password Manager, etc. Epic Games gave a free emote to users in Fortnite for tuning on 2sv and it went viral. We could give Play credit or G1.

## 5. Other random ideas that could help

These are various other areas we could invest in that would help. We should think about:

- 
- **Fixing unknown/incorrect age accounts.** We do not currently know who are kids (approx. [REDACTED] accounts are presumably used by underaged users). We therefore need to supercharge our age verification efforts (accelerate [REDACTED]).

- 
- 
- **Creating ads free/private paid Google/Google One:** For very privacy sensitive individuals, provide them an option through Google One to use Google Search & Chrome completely ads free.

- **Developing an IoT Privacy Master Switch:** Put all of your iot devices (cameras, speakers, hubs, etc) into private, no history mode with an Assistant privacy action or just one toggle from the Google App.

If you got this far, thank you for reading!

Your privacy obsessed pal...

L.



PRODBEG: GOOG-BRWN-00406065  
PRODBEGATT:  
PRODEND: GOOG-BRWN-00406070  
PRODENDATT:  
PRODVOL: PROD028  
2nd\_CROSS\_BEGBATES:  
2nd\_CROSS\_ENDBATES:  
AllCustodians: Rahul Roy-Chowdhury  
TO: luiz andré barroso <luiz@google.com>;rahul roy-chowdhury <rahulrc@google.com-  
>;sundar pichai <sundar@google.com>;jen fitzpatrick <jen@google.c-  
om>  
FROM: lorraine twohill <lorraine@google.com>  
CC:  
BCC:  
CONFIDENTIALITY: Confidential  
CROSS\_ALLCUSTODIANS:  
CROSS\_ATTACHMENTNAME:  
CROSS\_BEGATTACH:  
CROSS\_BEGBATES:  
CROSS\_CC:  
CROSS\_CONFIDENTIALITY:  
CROSS\_CUSTODIAN:  
CROSS\_DATECREATED:  
CROSS\_DATEMOD:  
CROSS\_DATERECEIVED:  
CROSS\_DATESENT:  
CROSS\_DE-DUPED CUSTODIANS:  
CROSS\_ENDATTACH:  
CROSS\_ENDBATES:  
CROSS\_FILEEXTENSION:  
CROSS\_FILENAME:  
CROSS\_FROM:  
CROSS\_MD5 HASH:  
CROSS\_MESSAGE ID:  
CROSS\_OWNER:  
CROSS\_PRODVAL:  
CROSS\_REDACTED:  
CROSS\_SUBJECT:  
CROSS\_TITLE:  
CROSS\_TO:  
CUSTODIAN/SOURCE: Rahul Roy-Chowdhury  
DATECREATED:  
DATELASTMOD: 01/29/2021  
DATERCVD:  
DATESENT:  
DeDupedCustodians:  
DOEXT:  
FILENAME:  
ILS\_ProdDate: 07/02/2021  
CROSS\_ILS\_ProdDate:  
MD5 HASH: 99F55195D647ECC203EFF542AC5B42E0  
MessageID:  
NATIVEFILE:  
Owner: lorraine  
PAGES:

REDACTED: N

SUBJECT: Today is Data Privacy day...so please read!

# Mao Declaration

## Exhibit 4

Redacted Version of Document  
Sought to Be Sealed

GOOG-BRWN-00475063



## Message

**From:** palmer@google.com [palmer@google.com]  
**Sent:** 7/11/2018 4:44:17 PM  
**To:** palmer@google.com; jyasskin@google.com; estark@google.com; kenrb@google.com; ellyjones@google.com; agl@google.com; sleevi@google.com  
**Subject:** AAAA952KuYI-IULXO2v58wc

- **palmer@google.com** 2018-07-11T16:44:17.423Z

There's some interest in [REDACTED] again

- **palmer@google.com** 2018-07-11T16:44:36.620Z

Mozilla and IPT 2 have everyone what we can do (which is good)

- **Updated on** 2018-07-11T16:52:30.089Z

Mozilla and IPT 2 have everyone wondering what we can do (which is good)

- **palmer@google.com** 2018-07-11T16:44:45.067Z

but I remain not on-board with [REDACTED] per se

- **palmer@google.com** 2018-07-11T16:44:54.465Z

what do other people think?

- **jyasskin@google.com** 2018-07-11T16:45:08.462Z

Also <https://brave.com/tor-tabs-beta/>.

- <https://brave.com/tor-tabs-beta/>

- **Updated on** 2018-07-11T16:52:18.703Z

Also <https://brave.com/tor-tabs-beta/>.

- <https://brave.com/tor-tabs-beta/>

- **estark@google.com** 2018-07-11T16:45:10.704Z

"Mozilla and IPT 2 have everyone what we can do" <-- missing a word?

- **kenrb@google.com** 2018-07-11T16:49:13.034Z

the question is whether we should consider trying to add web anonymization to Incognito?

- **estark@google.com** 2018-07-11T16:49:30.440Z

- **estark@google.com** 2018-07-11T16:49:38.983Z

and is basically orthogonal?

- **palmer@google.com** 2018-07-11T16:51:51.768Z

Oh, sorry: \*wondering\* what we can do

- **palmer@google.com** 2018-07-11T16:52:12.512Z

@Emily Stark Yes. But, people are just brainstorming.

- **estark@google.com** 2018-07-11T16:53:06.993Z

@Mike West has lots of Thoughts on the ITP stuff, have you seen any of his docs/brainstorms already?

- **palmer@google.com** 2018-07-11T16:53:14.634Z

1 idea was to [REDACTED] (!!!). I was like, no.

- **kenrb@google.com** 2018-07-11T16:53:23.823Z

- **palmer@google.com** 2018-07-11T16:53:32.557Z

Yeah I joined the [REDACTED] list, if that's what you mean @Emily Stark

- **palmer@google.com** 2018-07-11T16:54:15.470Z

a fear is that too-good tracking prevention will just escalate the arms race and we'll end up in a Fingerprinting Nightmare World

- **ellyjones@google.com** 2018-07-11T16:54:16.981Z

We looked at this for Chrome OS many years ago also

- **palmer@google.com** 2018-07-11T16:54:20.311Z

yeah

- **estark@google.com** 2018-07-11T16:54:25.686Z

in a former life I worked on a project to bundle a node in every webpage ☺

- **ellyjones@google.com** 2018-07-11T16:54:31.290Z

and the [REDACTED] people hard passed on the idea of shipping a [REDACTED] node on each chromebook - it would have demolished their infra

- **ellyjones@google.com** 2018-07-11T16:54:49.786Z

(this was in like 2011 so maybe things have changed)

- **ellyjones@google.com** 2018-07-11T16:55:03.495Z

I know Sleeve has strong feelings about [REDACTED]

- **estark@google.com** 2018-07-11T16:55:45.126Z

@Chris Palmer I also fear the Prompt On Every Subresource For Every Webpage Nightmare World

- **kenrb@google.com** 2018-07-11T16:56:09.079Z

@Chris Palmer but maybe we can reduce fingerprinting vectors to the point where few people are individually distinguishable

- **ellyjones@google.com** 2018-07-11T16:56:19.715Z

"This website would like to load an image. [Allow] [Deny]"

- **agl@google.com** 2018-07-11T16:58:17.233Z

Clearly the answer is for the whole world to use AMP, then we can expose the AMP cache via a Private Information Retrieval protocol and disable Javascript when rendering.

- **palmer@google.com** 2018-07-11T16:59:15.671Z

that is... wow

- **palmer@google.com** 2018-07-11T16:59:25.640Z

If I weren't already sitting down, I'd need to sit down

- **jyasskin@google.com** 2018-07-11T17:00:45.654Z

I assume everyone's seen <https://www.blaseur.com/papers/www18privatebrowsing.pdf>? (Thanks @Martin Shelton)

- <https://www.blaseur.com/papers/www18privatebrowsing.pdf>

- **palmer@google.com** 2018-07-11T17:01:04.761Z

yep, I am waving it in front of people

- **palmer@google.com** 2018-07-11T17:01:36.786Z

I am going to get back on my old shit of yelling that we need to stop calling it Incognito and stop using a Spy Guy icon

- **palmer@google.com** 2018-07-11T17:01:40.468Z

Temporary Mode

- **palmer@google.com** 2018-07-11T17:02:27.381Z

although that paper does note that people were least confused by Chrome's disclosure (their word for the disclaimer/explainer language)

- **palmer@google.com** 2018-07-11T17:02:54.443Z

Incognito: Voted Least Confusing Private Mode, 2018

- **ellyjones@google.com** 2018-07-11T17:04:37.562Z

good news palmer

- **ellyjones@google.com** 2018-07-11T17:04:47.313Z

we're working on a Dark Mode for Mac Chrome that will probably look quite a bit like incognito

- **kenrb@google.com** 2018-07-11T17:05:32.947Z

call it 'Dark Web Mode'

- **ellyjones@google.com** 2018-07-11T17:05:50.778Z

I love it

- **palmer@google.com** 2018-07-11T17:06:44.351Z

sob

- **kenrb@google.com** 2018-07-11T17:07:04.006Z

@Chris Palmer I know the 'incognito' war was waged and lost years ago, but do you remember why? It has always been a misleading name

- **palmer@google.com** 2018-07-11T17:07:22.790Z

Just as long as we don't get a Dark Intellectual Web Mode

(<https://www.nytimes.com/2018/05/08/opinion/intellectual-dark-web.html>)

- <https://www.nytimes.com/2018/05/08/opinion/intellectual-dark-web.html>

- **ellyjones@google.com** 2018-07-11T17:07:40.746Z

regardless of the name, the icon should always have been [http://simpsons.wikia.com/wiki/Guy\\_Incognito](http://simpsons.wikia.com/wiki/Guy_Incognito)

- [http://simpsons.wikia.com/wiki/Guy\\_Incognito](http://simpsons.wikia.com/wiki/Guy_Incognito)

- **ellyjones@google.com** 2018-07-11T17:07:49.327Z

which also accurately conveys the level of privacy it provides I think

- **palmer@google.com** 2018-07-11T17:08:13.654Z

@Ken Buchanan They didn't believe me that people would get confused; and they were still loving the Aw, Snap!/i18n-resistant whimsy thing

- **palmer@google.com** 2018-07-11T17:08:17.227Z

Maybe now is the time

- **kenrb@google.com** 2018-07-11T17:08:37.081Z



I see

- **palmer@google.com** 2018-07-11T17:08:38.747Z

now that we have results from, among others, a person we offered an Enamel job to (Sascha Fahl, co-author)

- **kenrb@google.com** 2018-07-11T17:09:13.964Z

"We have this wall of text explaining to people that incognito doesn't mean unrecognizable, when we use it"

- **sleevi@google.com** 2018-07-11T20:03:52.557Z

Yes, Eric Roman has similarly Strong Feelings about [REDACTED]. In theory, I'm not opposed to [REDACTED]  
[REDACTED] is that it's  
largely un(der?)staffed. Between [REDACTED], things just get... really weird and unpredictable. I  
mean, same as Android, just more weird. [REDACTED]  
[REDACTED]

PRODBEG: GOOG-BRWN-00475063  
PRODBEGATT:  
PRODEND: GOOG-BRWN-00475066  
PRODENDATT:  
PRODVOL: PROD034  
2nd\_CROSS\_BEGBATES:  
2nd\_CROSS\_ENDBATES:  
AllCustodians: Google  
TO: estark@google.com;agl@google.com;kenrb@google.com;ellyjones@google.com;sleevi@google.com;jyasskin@google.com;palmer@google.com  
FROM: palmer@google.com  
CC:  
BCC:  
CONFIDENTIALITY: Confidential  
CROSS\_ALLCUSTODIANS: Google  
CROSS\_ATTACHMENTNAME:  
CROSS\_BEGATTACH:  
CROSS\_BEGBATES: GOOG-CABR-00796941  
CROSS\_CC:  
CROSS\_CONFIDENTIALITY: CONFIDENTIAL  
CROSS\_CUSTODIAN: Google  
CROSS\_DATECREATED:  
CROSS\_DATEMOD: 07/11/2018  
CROSS\_DATERECEIVED: 07/11/2018  
CROSS\_DATESENT: 07/11/2018  
CROSS\_DE-DUPED CUSTODIANS: Google  
CROSS\_ENDATTACH:  
CROSS\_ENDBATES: GOOG-CABR-00796944  
CROSS\_FILEEXTENSION: eml  
CROSS\_FILENAME:  
CROSS\_FROM: palmer@google.com  
CROSS\_MD5 HASH: 88A12331DC1EF016C90A8C96F4611710  
CROSS\_MESSAGE ID: <AAAA952KuYI-IULXO2v58wc>  
CROSS\_OWNER: palmer  
CROSS\_PRODVAL: CROSS-PROD002  
CROSS\_REDACTED: N  
CROSS\_SUBJECT: AAAA952KuYI-IULXO2v58wc  
CROSS\_TITLE: AAAA952KuYI-IULXO2v58wc  
CROSS\_TO: estark@google.com;agl@google.com;kenrb@google.com;ellyjones@google.com;sleevi@google.com;jyasskin@google.com;palmer@google.com  
CUSTODIAN/SOURCE: Google  
DATECREATED:  
DATELASTMOD: 07/11/2018  
DATERCVD:  
DATESENT: 07/11/2018  
DeDupedCustodians:  
DOEXT:  
FILENAME:  
ILS\_ProdDate: 08/13/2021  
CROSS\_ILS\_ProdDate: 09/01/2021  
MD5 HASH: 88A12331DC1EF016C90A8C96F4611710  
MessageID:  
NATIVEFILE:  
Owner:  
PAGES:

REDACTED: N

SUBJECT: AAAA952KuYI-IULXO2v58wc

# Mao Declaration

## Exhibit 5

Redacted Version of Document  
Sought to Be Sealed

GOOG-CABR-00084985



# Chrome and the Shifting Privacy and Security Landscape



[martinshelton@](mailto:martinshelton@)

Slides: [go/chrome-sp-landscape](https://go/chrome-sp-landscape)

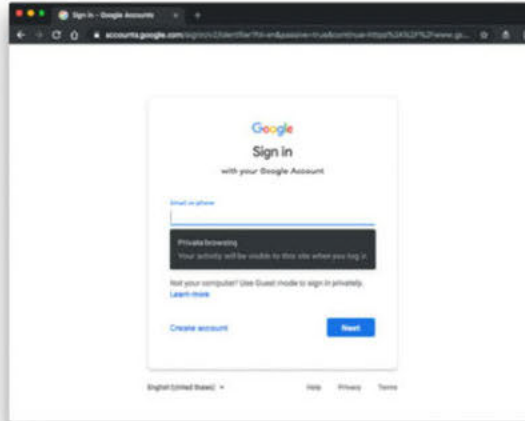
December 2018

GOOGLE CONFIDENTIAL AND PROPRIETARY

## More privacy ideas: Be cautioned what is and isn't private with Incognito

We know users have a tough time understanding how Incognito works, and [several common misconceptions](#). The same is true for private browsing more generally.

What if we gave users contextual hints, so they can understand Incognito's limitations when they need it? - maxwalker@



GOOGLE CONFIDENTIAL AND PROPRIETARY

Via maxwalker@. See our Incognito brainstorm deck:



Check out rhalavati@'s Incognito user education PRD:



PRODBEG: GOOG-CALH-00031543  
PRODBEGATT:  
PRODEND: GOOG-CALH-00031605  
PRODENDATT:  
PRODVOL: CROSS-PROD002  
2nd\_CROSS\_BEGBATES:  
2nd\_CROSS\_ENDBATES:  
AllCustodians: Google  
TO:  
FROM:  
CC:  
BCC:  
CONFIDENTIALITY: CONFIDENTIAL  
CROSS\_ALLCUSTODIANS:  
CROSS\_ATTACHMENTNAME:  
CROSS\_BEGATTACH:  
CROSS\_BEGBATES: GOOG-CABR-00084985  
CROSS\_CC:  
CROSS\_CONFIDENTIALITY:  
CROSS\_CUSTODIAN:  
CROSS\_DATECREATED:  
CROSS\_DATEMOD:  
CROSS\_DATERECEIVED:  
CROSS\_DATESENT:  
CROSS\_DE-DUPED CUSTODIANS:  
CROSS\_ENDATTACH:  
CROSS\_ENDBATES: GOOG-CABR-00085047  
CROSS\_FILEEXTENSION:  
CROSS\_FILENAME:  
CROSS\_FROM:  
CROSS\_MD5 HASH:  
CROSS\_MESSAGE ID:  
CROSS\_OWNER:  
CROSS\_PRODVAL:  
CROSS\_REDACTED:  
CROSS\_SUBJECT:  
CROSS\_TITLE:  
CROSS\_TO:  
CUSTODIAN/SOURCE: Google  
DATECREATED: 03/04/2021  
DATELASTMOD: 03/04/2021  
DATERCVD:  
DATESENT:  
DeDuplicatedCustodians: Google  
DOEXT: PPTX  
FILENAME: Chrome\_and\_the\_Shifting\_Privacy\_and\_Security\_Landscape.pptx  
ILS\_ProdDate: 09/01/2021  
CROSS\_ILS\_ProdDate: 09/01/2021  
MD5 HASH: 062AA316C77842A8C43F87468C5F8026  
MessageID:  
NATIVEFILE:  
Owner:  
PAGES: 63  
REDACTED: N  
SUBJECT:

# Mao Declaration

## Exhibit 9

Sealed Entirely

GOOG-CABR-00093167



# Mao Declaration

## Exhibit 10

Redacted Version of Document  
Sought to Be Sealed

GOOG-BRWN-00388293

## Message

**From:** Mardini [mardini@google.com]  
**Sent:** 4/30/2019 7:14:16 PM  
**To:** Jochen Eisinger [eisinger@google.com]; Shimi Rahim [srahim@google.com]  
**CC:** Margret Schmidt [margrets@google.com]; Parisa Tabriz [parisa@google.com]; Alex Ainslie [ainslie@google.com]  
**Subject:** Re: Branding for Incognito (IO Update)

[narrowing down list of recipients - pls don't forward]

An update on our meeting with Sammit today. We discussed the following:

- 1/ Debugging the process
- 2/ Got context around the incognito iconography/rebranding for I/O then cancellation
- 3/ Got clarity on who owns that Incognito comms doc and whether our comments are being addressed

1/ Made it clear what the ideal process should be from Chrome's point of view. No disagreements there and it was clear for them but there was a mad rush to get things for I/O from various execs that made folks panic.

2/ This was driven by Lorraine who told the PDPO steering committee that Incognito might need rebranding so a workstream ensued involving the brand studio about 2-3 weeks ago.

Yesterday, at the PDPO SC meeting, Tom Oliveri was present and told them that Sundar didn't want to put incognito under the spotlight so this iconography/rebranding should not be an I/O topic.

The plan of record with regards to incognito in I/O is just to mention in one or two sentences related to bringing Incognito to Google Maps (not clear whether there will be mocks or not for that).

The SC was asked to commit to exploring in 2019 to develop a consistent vision for how an "Incognito 2.0" would look like with impact analysis on revenue, usage, and comms.

Relatedly, Ben Gomes showed a demo of AGSA launching Chrome in Incognito mode. i.e. if a user is in AGSA and they want to conduct an incognito search, they'd intent into an Incognito NTP in Clank

3/ That comms doc is owned by the brand studio and Sundar's speech writing team. I emphasized the need to double check with Chrome PM/Eng the accuracy of the information mentioned there. Sammit acknowledged but mentioned that the comms around I/O are very closely guarded and it's challenging to get a full picture for what will be said exactly....

Thanks,

--Mardini

On Tue, Apr 30, 2019 at 8:40 AM Mardini <mardini@google.com> wrote:

Le mar. 30 avr. 2019 à 08:33, Mardini <mardini@google.com> a écrit :

Thank you, Alex.

We (Rory/Ramin/Sabine/myself) have a meeting with Sammit today so will discuss the process and work cadence issue as well.

As discussed in our chat yesterday, Jochen and I will try to get some time with the PDPO folks visiting Munich for GSEC in a couple of weeks to sync in person.

I also didn't receive the note below about revisiting the incognito brand after I/O. Maybe it was sent only to those who replied "yes" to the meeting.

I see it now. Gmail didn't classify it as important :/.

Le mar. 30 avr. 2019 à 07:29, Yuan Chen <[yuanchen@google.com](mailto:yuanchen@google.com)> a écrit :

Thank you for keeping us in the loop - I also didn't get the update from PDPO. I agree we need to get into a better work cadence with PDPO folks.

On Tue, Apr 30, 2019 at 2:12 AM Shimi Rahim <[srahim@google.com](mailto:srahim@google.com)> wrote:

Thanks for filling us in, Alex & Parisa (I didn't see an email from PDPO), and for helping us navigate I/O challenges!

On Mon, Apr 29, 2019 at 5:03 PM Parisa Tabriz <[parisa@google.com](mailto:parisa@google.com)> wrote:

On Mon, Apr 29, 2019 at 4:42 PM Alex Ainslie <[ainslie@google.com](mailto:ainslie@google.com)> wrote:  
(narrowing to just Chrome folks)

I'm glad to see the update from PDPO below about waiting to tackle any branding updates until After IO.

Ah, me too!

Their timing was too aggressive and their proposal wasn't compelling :/

Here's the Chrome summary from my discussions with many of you (in sequence) this morning:

- Chrome is comfortable with a high level message at IO about expanding Incognito to other flagship Google products on Android (AGSA, Maps, YouTube).
- We've nurtured the Incognito brand for the past 10 years and our team would need to conduct a significant investigation (including UX Research) to feel confident about a change.
- For that reason, Chrome does not support announcing new PDPO-proposed branding at IO
- Additionally, speculative announcements related to Privacy are extra risky because the bar for Google is high and we need to make sure not to promise something we can't deliver.

#### Chrome + PDPO (Mis)alignment

Should Google ...	PDPO + Brand Studio	Chrome
... do more product work focused on Privacy?	Yes	Yes
... talk more about that Privacy work in public?	Yes	Yes
... extend Chrome's Incognito mode to other products?	Yes	Maybe?
... change the current Incognito brand?	Yes	Maybe? Err
... announce Incognito branding changes at IO before they've been thoroughly studied?	Yes	No

Going forward, I agree with Jochen that we'll need to get into a better working cadence with PDPO folks.

Yep. I'd recommend syncing with [miraglia@](mailto:miraglia@) in a small setting to share how this effort was perceived from the Chrome side so we can reset.

Alex

On Mon, Apr 29, 2019 at 4:00 PM Sammit Adhya <[sadhya@google.com](mailto:sadhya@google.com)> wrote:

Hi Everyone,

Just wanted to let you know that leads decided to revisit the Incognito branding after I/O. Apologies for scheduling the urgent meeting, but we look forward to working with everyone after I/O.

Thanks much,

Sammit

## **[Confirmed] - Exploration of Iconography and Branding for Incognito**

### ***Scheduled per Sammit's request***

We wanted to share some new Incognito branding and iconography ideas that the Brand Studio team has been exploring to get your thoughts and feedback.

Leads: anilsa, parisa, miraglia

PM: (rorymccllland), (sabineb), mardini

Eng: eisinger, (rhalavati)

UXR: martinshelton, (lorindole)

UXD: ainslie

Marketing: martinal, jcroom

Brand: mediha, julianneyi, frederick

PDPO: sadhya, gregfair, rast

When Tue Apr 30, 2019 3:30pm – 4pm Pacific Time - Los Angeles

Where MTV-900-2-ChromeOZone (8) [GVC, No External Guests], MTV-900-2-Rage Against The Machine (4) [GVC, No External Guests], SFO-1MST-14-Daniel Handler (4) [GVC], SFO-2HS-4-Eight O'Clock Coffee (5) [GVC], SYD-ODI-3-410 - Gone (2) [GVC, No External Guests, Phone] ([map](#))

Joining info

[REDACTED]

[REDACTED] [More phone numbers](#)

Who

- Eric Miraglia - organizer
- Jieun Lee - creator
- Martin Shelton
- Sammit Adhya
- [rast@google.com](mailto:rast@google.com)
- Martina Laresova
- Ken Frederick
- Jochen Eisinger
- James Croom
- Anil Sabharwal
- Mediha Abdulhay
- Greg Fair
- Alex Ainslie
- Shimi Rahim
- AbdelKarim Mardini
- Martha Welsh
- Julianne Yi
- Parisa Tabriz



- Ramin Halavati - optional
- Lorin Dole - optional
- Sabine Borsay - optional
- Rory McClelland - optional

--

**Yuan Chen**

Interaction Designer

Google Germany GmbH

Erika-Mann-Str. 33

80636 München

Geschäftsführer: Paul Menole, Hallimah DeLaine Prado  
Registrierungs- und -nummer: Hamburg, HRB 88881  
Sitz der Gesellschaft: Hamburg

Diese E-Mail ist vertraulich. Wenn Sie nicht der richtige Adressat sind, sollen Sie diese bitte nicht weiter, informieren Sie den Absender und löschen Sie die E-Mail und alle Anhänge. Vielen Dank.

This e-mail is confidential. If you are not the right addressee please do not forward it, please inform the sender, and please erase this e-mail including any attachments. Thanks.

PRODBEG: GOOG-BRWN-00388293  
PRODBEGATT:  
PRODEND: GOOG-BRWN-00388296  
PRODENDATT:  
PRODVOL: PROD028  
2nd\_CROSS\_BEGBATES:  
2nd\_CROSS\_ENDBATES:  
AllCustodians: AbdelKarim Mardini  
TO: jochen eisinger <eisinger@google.com>;shimi rahim <srahim@google.com>  
FROM: mardini <ardini@google.com>  
CC: parisa tabriz <parisa@google.com>;alex ainslie <ainslie@google.com>;margret  
schmidt <margrets@google.com>  
BCC:  
CONFIDENTIALITY: Confidential  
CROSS\_ALLCUSTODIANS: AbdelKarim Mardini  
CROSS\_ATTACHMENTNAME:  
CROSS\_BEGATTACH:  
CROSS\_BEGBATES: GOOG-CABR-00224709  
CROSS\_CC: parisa tabriz <parisa@google.com>;alex ainslie <ainslie@google.com>;ma-  
rgret schmidt <margrets@google.com>  
CROSS\_CONFIDENTIALITY: CONFIDENTIAL  
CROSS\_CUSTODIAN: AbdelKarim Mardini  
CROSS\_DATECREATED:  
CROSS\_DATEMOD: 04/30/2019  
CROSS\_DATERECEIVED: 04/30/2019  
CROSS\_DATESENT: 04/30/2019  
CROSS\_DE-DUPED CUSTODIANS: AbdelKarim Mardini  
CROSS\_ENDATTACH:  
CROSS\_ENDBATES: GOOG-CABR-00224712  
CROSS\_FILEEXTENSION: eml  
CROSS\_FILENAME:  
CROSS\_FROM: mardini <ardini@google.com>  
CROSS\_MD5 HASH: 1965D5D98ACCB9D49C7EBD0CFECB78E2  
CROSS\_MESSAGE ID: <CAGQY0Od-g=UK1G7bexQVsaig5aiu+i5wd4edce\_3x+VoeBtV8w@mail.gmai-  
l.com>  
CROSS\_OWNER: mardini  
CROSS\_PRODVAL: CROSS-PROD002  
CROSS\_REDACTED: N  
CROSS\_SUBJECT: Re: Branding for Incognito (IO Update)  
CROSS\_TITLE: Re: Branding for Incognito (IO Update)  
CROSS\_TO: jochen eisinger <eisinger@google.com>;shimi rahim <srahim@google.com>  
CUSTODIAN/SOURCE: AbdelKarim Mardini  
DATECREATED:  
DATELASTMOD: 04/30/2019  
DATERCVD:  
DATESENT:  
DeDupedCustodians:  
DOEXT:  
FILENAME:  
ILS\_ProdDate: 07/02/2021  
CROSS\_ILS\_ProdDate: 09/01/2021  
MD5 HASH: 1965D5D98ACCB9D49C7EBD0CFECB78E2  
MessageID:  
NATIVEFILE:  
Owner: mardini

PAGES:

REDACTED: N

SUBJECT: Re: Branding for Incognito (IO Update)

# Mao Declaration

## Exhibit 12

Redacted Version of Document  
Sought to Be Sealed

GOOG-BRWN-00140297

# The Incognito Problem

Chris Palmer (palmer@)



Key Fact:  
Incognito  
Confuses People

## "Incognito" Confuses People

We know from intuition, anecdotes, and now empirically ([Yuxi Wu, et al.](#); see also [Habib, et al.](#)) that the "incognito"/Spy Guy branding, and the complex disclosures (like all complex disclosures), confuse people as to what exact guarantees it offers and does not offer.

Ironically, across all browsers, Chrome's disclosures were the least confusing by a modest amount. But it's still bad.

Id	Date	Text
1	07/22/2018 07:53:36	It'd be good to try to replicate or further validate the study, but I'd be surprised if we got a significantly different result.

WWW 2018, April 23–27, 2018, Lyon, France

Yuxi Wu, Panya Gupta, Miranda Wei, Yasemin Acar<sup>†</sup>, Sascha Fahl<sup>†</sup>, Blase Ur

**Table 5: Scenarios where participants held misconceptions, shown with the correct answers and percentage of participants who gave incorrect answers. For comparative scenarios, (in)equality symbols denote the correct answer, and we give the sum of all participants answering otherwise.**

Scenario	Answer		% Incorrect	
	Std.	Priv.	Std.	Priv.
<i>Overestimating private mode's privacy protections</i>				
Search queries associated (logged in)	Yes	Yes	1.5	56.3
Bookmarks saved across sessions	Yes	Yes	25.4	46.5
Geolocation can be estimated	Yes	Yes	5.2	40.2
Employer can track browsing	Yes	Yes	1.1	37.0
Better protected from viruses/malware	Std. = Priv.		27.1	
IP address can be collected	Yes	Yes	0.7	25.2
Government can track browsing	Yes	Yes	4.1	22.6
ISP can track browsing	Yes	Yes	3.0	22.0
<i>Underestimating private mode's privacy protections</i>				
Downloaded file in browser's list	Yes	No <sup>a</sup>	1.3	51.7
Proportion of targeted ads	Std. > Priv.		30.9	
Search queries associated (not logged in)	Yes	No	20.2	30.0

<sup>a</sup>Except in Brave's private mode, which does retain download history

**Table 6: Distinguishing scenarios where private mode's impact depends on the browser or context.**

Scenario	% Yes	
	Std.	Priv.
Items in shopping cart saved across sessions	97.8	78.8
Browser extensions active across sessions	98.3	69.1
Forensic expert can reconstruct browsing history	98.7	52.8
Site-specific preferences (e.g., for pop-ups) saved	98.3	31.3

**Table 7: Distribution of responses for comparative scenarios where the impact depends on the browser or context.**

Scenario	% Responses		
	Std. > Priv.	Std. = Priv.	Std. < Priv.
Amount of ads	32.2	64.9	2.9
Page loading speed	24.8	53.6	21.6

( $\chi^2(12) = 38.1, p = .001$ ). In the control condition, 32.4% of participants mistakenly believed downloaded files would still be listed in the browser. A higher proportion of participants in Brave (62.2%,

## This Is Bad

**We are over-promising and under-delivering.**

This is bad for people and reflects badly on our product when/if people do come to understand.



Key Question:  
What Do People  
Use Incognito  
For?

## Why Do People Use Private Modes?

From Wu, et al.:

1. Hide browsing history, especially visits to adult websites;
2. prevent targeted ads and search suggestions;
3. achieve "safer" browsing;
4. Prevent browsers from saving login-related information;
5. avoid cookies;
6. accommodate intentional or unintentional use by others.

Id	Date	Text
1	07/23/2018 13:28:04	what's the motivation here? how does this differ from 2?
2	07/23/2018 13:28:04	This is a list of reasons that people reported to the researchers for why they use private browsing modes. Part of the point of the research is that people don't fully understand the mechanisms.

## Incognito Is Overloaded

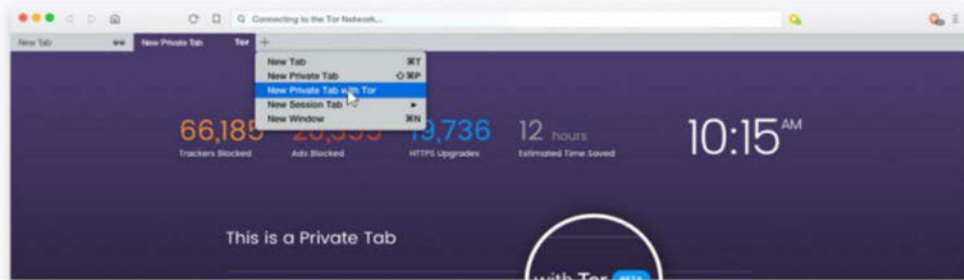
Those 6 reasons are related but different. Perhaps we really need multiple modes (we've already got Guest mode)?

Or more and easier affordances for privacy and control in Settings/elsewhere?

Key Fact: There's  
A Privacy Feature  
Race

# Brave Introduces Beta of Private Tabs with Tor for Enhanced Privacy while Browsing

by Brave | Jun 28, 2018 | Announcements, Features, Privacy





## A Firefox Competitive Advantage

The Tor Project developers said that Project Fusion has the accord of Mozilla's CEO and CTO, which probably means it has a high chance of coming to fruition. However, many issues have to be considered first, such as developing private telemetry, fixing the problem with fingerprinting resistance breaking websites, and so on.

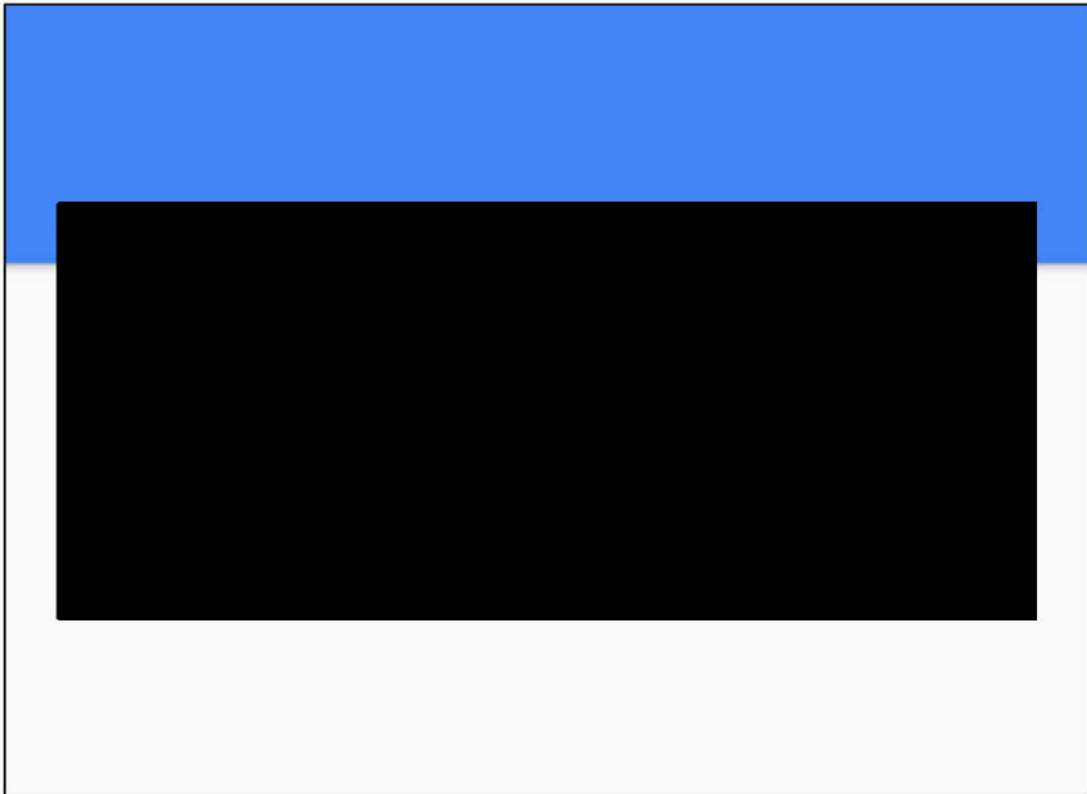
Additionally, Mozilla wants to first standardize the Tor client specification, write conformance tests for it, and open the documentation. All of that means that more people could look at how Tor is implemented in Firefox and see if there are any issues with that implementation.

The main reason why Mozilla would even want to integrate Tor into Firefox is because it could provide its users real private browsing, something that most competitors will not be able to offer. Mozilla has taken an increasingly strong pro-privacy stance in the past few years, and Project Fusion could further boost its pro-privacy image.

It could also put Firefox in a much more direct contrast with Chrome, a browser developed by Google, which is heavily invested in user tracking in order to serve more targeted ads.

## ITP, ITP2, ITP3

Safari and Mozilla are moving in this area, and we'll need to have some kind of response as well.

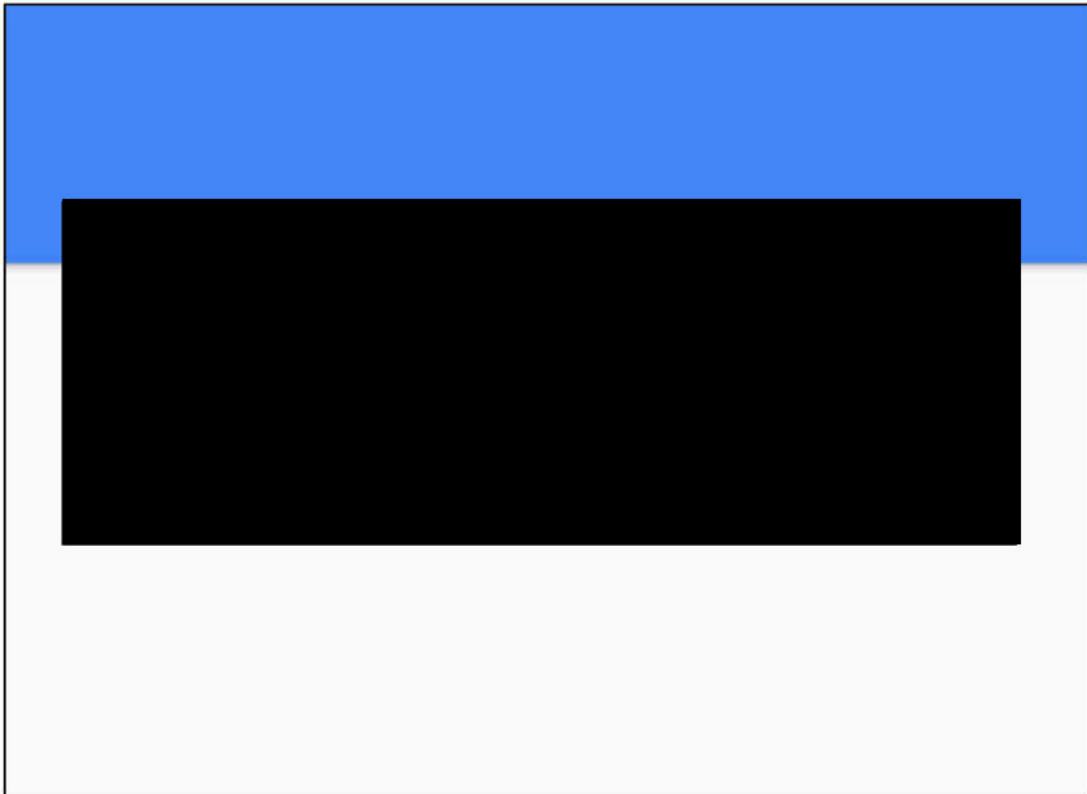


Id	Date	Text
1	07/21/2018 14:10:10	





Options

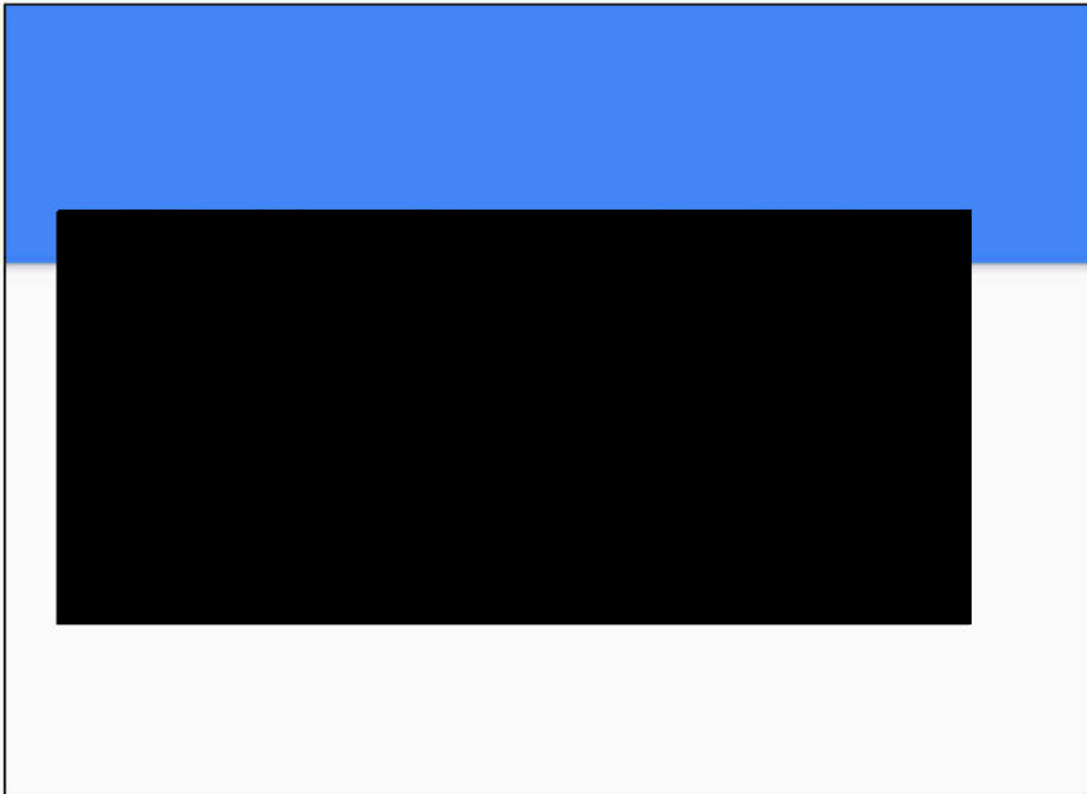


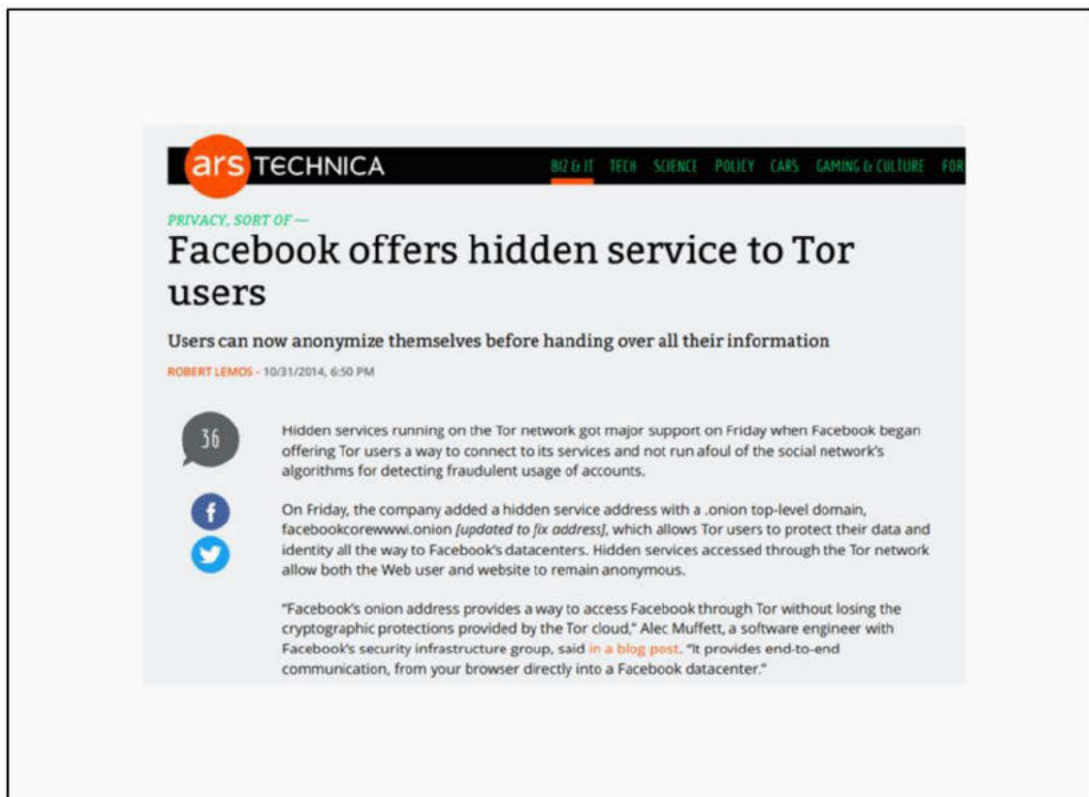


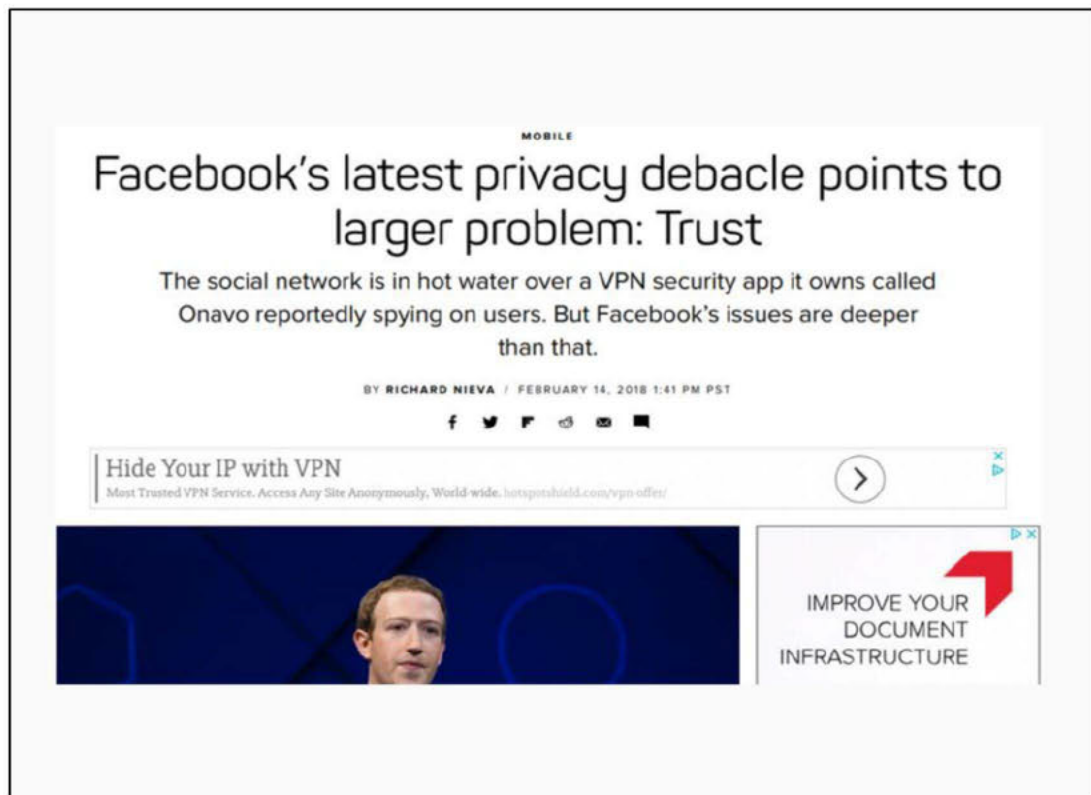


Id	Date	Text
1	07/23/2018 14:04:19	
1	07/23/2018 14:05:29	
2	07/23/2018 14:05:29	









## Most VPN Services are Terrible

Short version: I strongly *do not* recommend using any of these providers. You are, of course, free to use whatever you like. My TL;DR advice: Roll your own and use [Algo](#) or [Streisand](#). For messaging & voice, use [Signal](#). For increased anonymity, use [Tor](#) for desktop (though recognize that doing so may actually [put you at greater risk](#)), and [Onion Browser](#) for mobile.

This mini-rant came on the heels of an interesting twitter discussion:  
<https://twitter.com/kennwhite/status/591074055018582016>

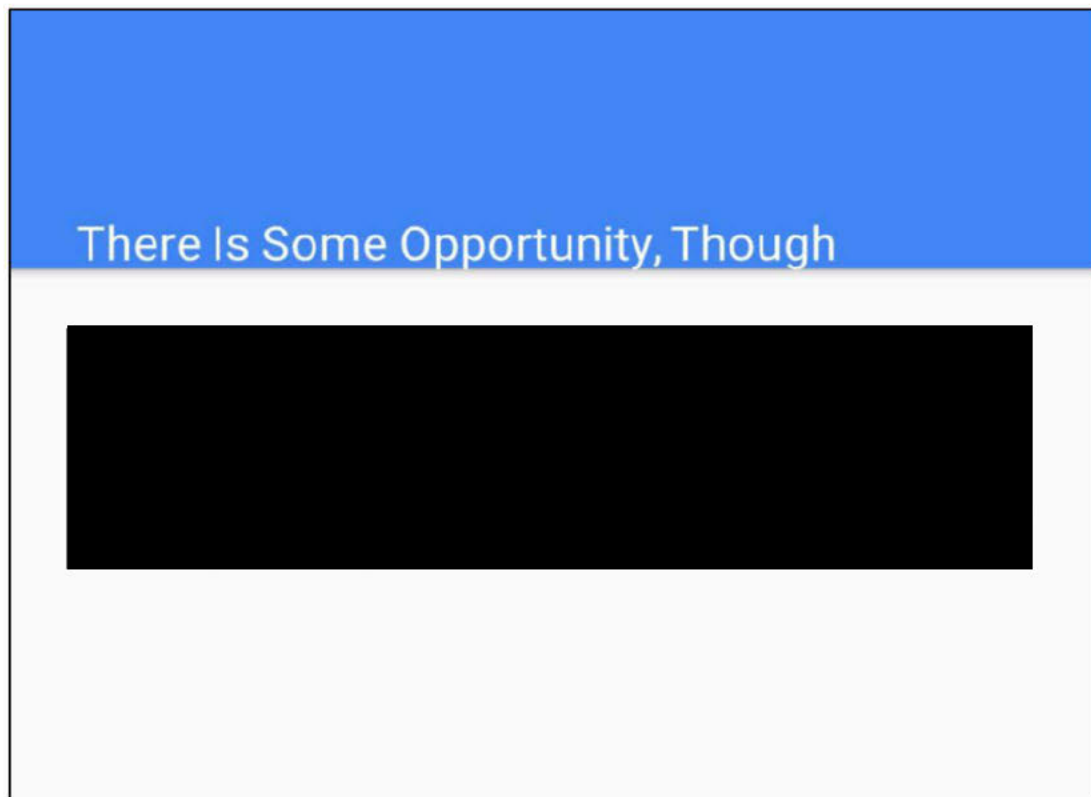
Again I strongly *do not* recommend using any of these providers.

Provider / known "Secret" Key

```
Astril / way2stars
EarthVPN / earthvpn
GFWVPN / gfwvpn
GoldenFrog / thisisourkey
IBVPN / ibVPNsharedPSK!
IPVanish / ipvanish
NordVPN / nordvpn
PrivateInternetAccess (PIA) / mysafety
PureVPN / 12345678
SlickVPN / gogoVPN
TorGuard / torguard
TigervPN / tigervPN
```


source: <https://gist.github.com/kennwhite/1f3bc4d889b02b35d8aa>



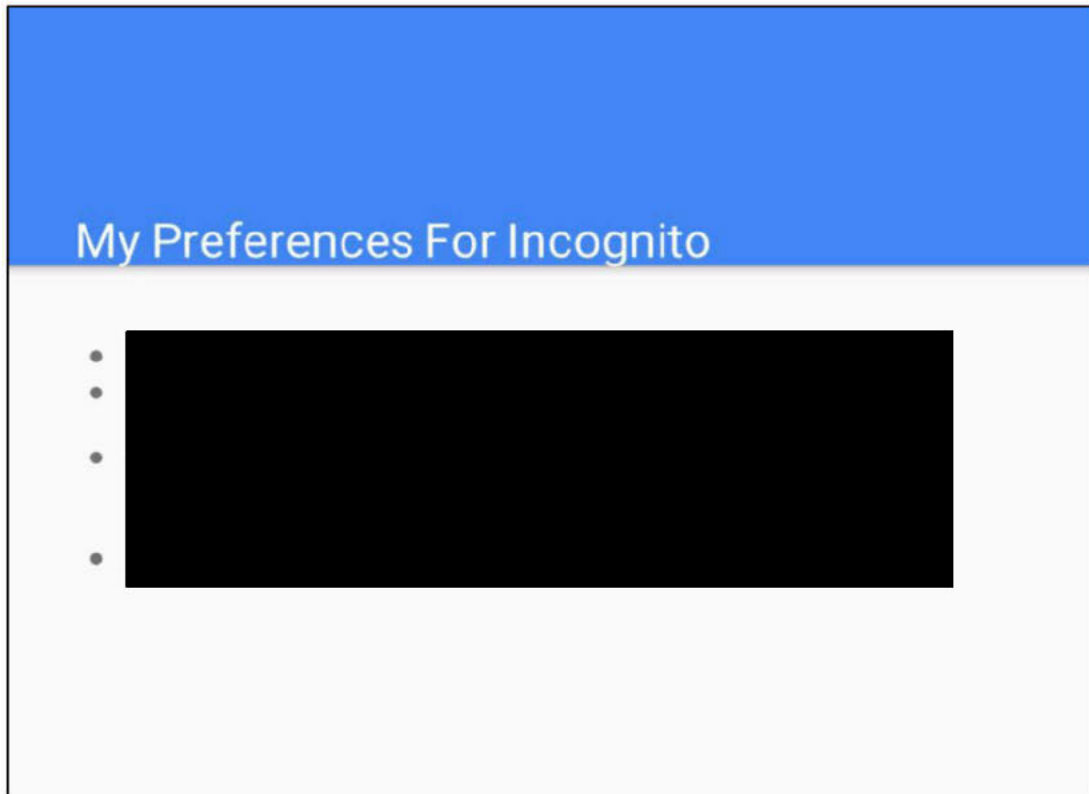


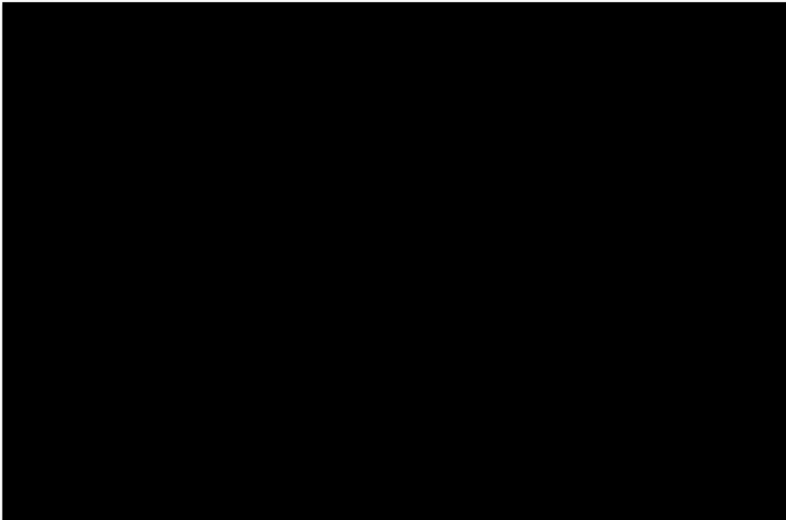
Key Question:  
How Much  
Breakage Will  
People Tolerate?

## Hypothesis: Not Much



Conclusion:  
Options, But No  
Single Clear Path



Id	Date	Text
1	07/21/2018 15:50:53	
3	07/22/2018 08:00:43	
2	07/23/2018 12:54:42	
3	07/23/2018 12:54:42	

## Additional Useful Efforts

- [REDACTED]
- [REDACTED]



PRODBEG: GOOG-BRWN-00140297  
PRODBEGATT:  
PRODEND: GOOG-BRWN-00140329  
PRODENDATT:  
PRODVOL: PROD023  
2nd\_CROSS\_BEGBATES:  
2nd\_CROSS\_ENDBATES:  
AllCustodians: AbdelKarim Mardini;Alexei Svitkine;Helen Harris  
TO:  
FROM:  
CC:  
BCC:  
CONFIDENTIALITY: Confidential  
CROSS\_ALLCUSTODIANS: AbdelKarim Mardini;Alexei Svitkine;Helen Harris  
CROSS\_ATTACHMENTNAME:  
CROSS\_BEGATTACH:  
CROSS\_BEGBATES: GOOG-CABR-00094818  
CROSS\_CC:  
CROSS\_CONFIDENTIALITY: CONFIDENTIAL  
CROSS\_CUSTODIAN: Alexei Svitkine  
CROSS\_DATECREATED: 07/21/2018  
CROSS\_DATEMOD: 10/09/2019  
CROSS\_DATERECEIVED:  
CROSS\_DATESENT:  
CROSS\_DE-DUPED CUSTODIANS: AbdelKarim Mardini;Alexei Svitkine;Helen Harris  
CROSS\_ENDATTACH:  
CROSS\_ENDBATES: GOOG-CABR-00094850  
CROSS\_FILEEXTENSION: pptx  
CROSS\_FILENAME: The Incognito Problem\_1TNOMivlbk0cAiQqY4twyccyjRYGHdry4vVWjt1h0-t4.pptx  
CROSS\_FROM:  
CROSS\_MD5 HASH: D073B8D9E8F4A04FB597F6D6AD115E38  
CROSS\_MESSAGE ID:  
CROSS\_OWNER: palmer@google.com  
CROSS\_PRODVAL: CROSS-PROD002  
CROSS\_REDACTED: N  
CROSS\_SUBJECT:  
CROSS\_TITLE: The Incognito Problem  
CROSS\_TO:  
CUSTODIAN/SOURCE: Alexei Svitkine  
DATECREATED: 07/21/2018  
DATELASTMOD: 10/09/2019  
DATERCVD:  
DATESENT:  
DeDupedCustodians:  
DOEXT:  
FILENAME: The Incognito Problem\_1TNOMivlbk0cAiQqY4twyccyjRYGHdry4vVWjt1h0t4.ppt-x  
ILS\_ProdDate: 06/18/2021  
CROSS\_ILS\_ProdDate: 09/01/2021  
MD5 HASH: D073B8D9E8F4A04FB597F6D6AD115E38  
MessageID:  
NATIVEFILE:  
Owner: palmer@google.com  
PAGES:

REDACTED: N  
SUBJECT:

# Mao Declaration

## Exhibit 14

Sealed Entirely

GOOG-BRWN-00490767

# Mao Declaration

## Exhibit 18

Sealed Entirely

GOOG-CABR-05836882

# Mao Declaration

## Exhibit 21

Sealed Entirely

GOOG-CABR-04154452

# Mao Declaration

## Exhibit 24

Redacted Version of  
Document Sought to Be Sealed

GOOG-CABR-05766200.R



Privileged and Confidential

# Incognito NTP Revamp PRD

Last updated: November 2021

Status: Draft | WIP | Ready to go | Done

Author(s)	<u>Andrew Kamau</u>
Leads	PM - <u>Andrew Kamau</u> UXD - <u>Peter Dijkgraaf</u> TL - <u>Ramin Halavati</u>
Project Team	<u>chrome-incognito@google.com</u>
Area Leads	PM - mardini@ (sabineb@), Eng - eisinger@, UX - jaroner@
Stakeholders	Legal, PR/Marketing
Useful Links	<u>NTP Revamp UI Review deck</u>   <u>Incognito 2021+ roadmap</u>   <u>Incognito success metrics</u>   <u>go/incognito-mission</u>   <u>Incognito insights</u>   <u>go/five-misunderstandings-incognito</u>   <u>User education exploration</u>   <u>Legal analysis</u>

## Background

We want users to be clear on what Incognito is designed to provide. There is an opportunity to clear up known user misconceptions and proactively educate users about Incognito.

This is a proposal on the first steps towards using the NTP to foster clearer user comprehension on what Incognito does (and does not do).

## Problem

Feedback from UXR indicates that users have misconceptions about Incognito and often overestimate the protections available. We want to help them clearly understand the scope of the elevated privacy protections on Incognito.

As a user, I want to have an **easy to use** and **understandable** way to temporarily browse the web with elevated privacy.

## Goal

This project feeds into one of our top priorities as represented in Chrome BrApp 2021 OKRs and Incognito 2021 roadmap: **Clear up user confusion** around Incognito mode by investing more in clarity of user education.

## Non-goals

This PRD only captures the breadth of what can be done now (2021) considering the constraints on making far reaching changes on Incognito NTP. Therefore, it does not cover open questions and ideas that we might consider post-v1, including:

- Updating NTP strings. Due to legal constraints, the strings on revamped NTP **will not differ** much from what we have today.
- Settings & controls: NTP is **not a settings page**. IPH prompts may be used to direct users to specific settings.

## Success Metrics

While we are not tying this proposal to any quantitative usage metrics, we will keep an eye on possible second order effects on the key BEAT metrics tied to Incognito's vision:

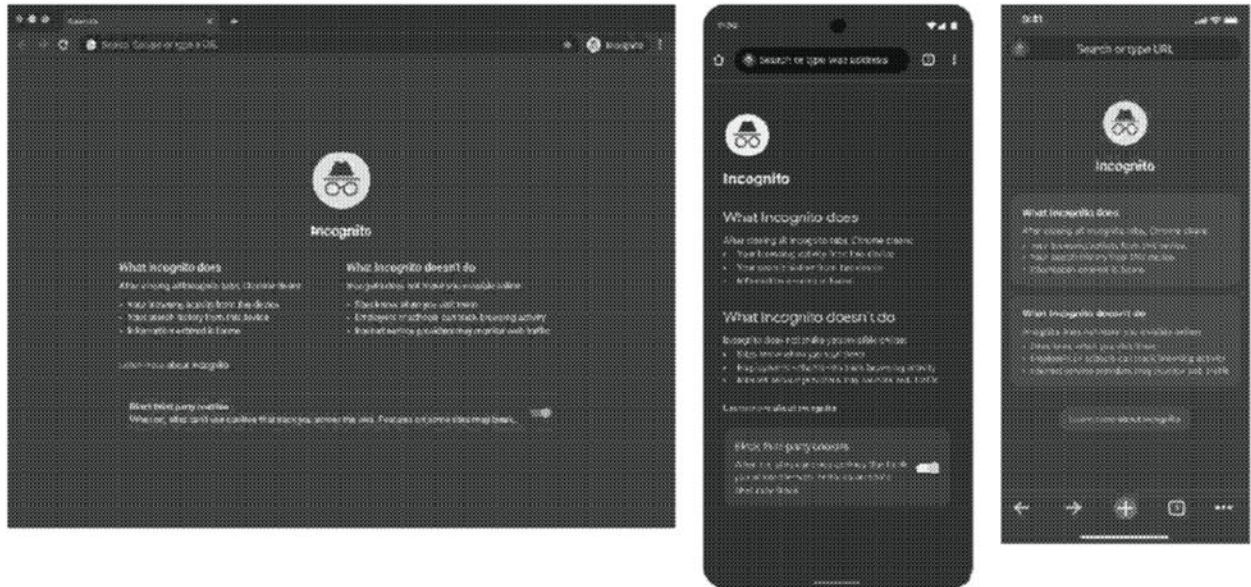
- Task success:
  - **Reduced misconceptions** as measured by qualitative surveys of users.
  - **Shortness of Incognito sessions**. Currently stands at an average of [REDACTED]
- Benovelence:
  - User trust in Chrome and Incognito as a privacy brand as measured in the brand tracker.

We'll also gather and evaluate direct user feedback from these changes, as well as opinions and reactions from the press.

## Proposal

The proposed solution is premised on the hypothesis that users will be better served by **increasing the scannability of the NTP pointers** describing what Incognito does and does not do.





*Proposed NTP on Desktop, Clank, and Bling*

## Considerations

### Legal

Redacted - Privilege

### Privacy

Incognito mode is Google's most used privacy brand. Product excellence changes like this are aimed at making our core Incognito promise more trustworthy and predictable. With that, they contribute to making Chrome's privacy story stronger.

Redacted - Privilege

# Redacted - Privilege

Privacy review guidance:

# Redacted - Privilege

## UX

Recognizing that the NTP is an entry point (a step - not a goal - in the CUJ), it needs to strike the balance between information density and scannability.

On mobile, the illustrations are removed in order to prevent the text from being pushed below the fold.

[More UX explorations.](#)

## UXW

[go/incognito-strings](#)

Other surfaces that borrow from Incognito NTP:

- [AGA interstitial](#)
- [Help centre article](#)

## gTech

Proposed help centre article updates: [M98: Incognito NTP Revamp | Help Centre Updates by gTech](#)

## Marketing & PR

As we approach the target launch milestone, we'll consider alignment with the narrative around related efforts for a stronger marketing moment:



Reactive comms write-up.

## Open issues and risks

Cross-platform alignment on the implementation might impact the scope of this project.

- How does the UI layout on mobile scale to desktop?
- What's the 3rd party cookie toggle placement on mobile?

## Milestones

Targeting M97

## Decision Log

Date	Decision	Participants (@ each one)
7/13/2021	Approved	sabineb@

PRODBEG: GOOG-CABR-05766200  
PRODBEGATT:  
PRODEND: GOOG-CABR-05766204.R  
PRODENDATT:  
PRODVOL: CROSS-PROD082  
2nd\_CROSS\_BEGBATES:  
2nd\_CROSS\_ENDBATES:  
AllCustodians: Google  
TO:  
FROM:  
CC:  
BCC:  
CONFIDENTIALITY: CONFIDENTIAL  
CROSS\_ALLCUSTODIANS:  
CROSS\_ATTACHMENTNAME:  
CROSS\_BEGATTACH:  
CROSS\_BEGBATES:  
CROSS\_CC:  
CROSS\_CONFIDENTIALITY:  
CROSS\_CUSTODIAN:  
CROSS\_DATECREATED:  
CROSS\_DATEMOD:  
CROSS\_DATERECEIVED:  
CROSS\_DATESENT:  
CROSS\_DE-DUPED CUSTODIANS:  
CROSS\_ENDATTACH:  
CROSS\_ENDBATES:  
CROSS\_FILEEXTENSION:  
CROSS\_FILENAME:  
CROSS\_FROM:  
CROSS\_MD5 HASH:  
CROSS\_MESSAGE ID:  
CROSS\_OWNER:  
CROSS\_PRODVAL:  
CROSS\_REDACTED:  
CROSS\_SUBJECT:  
CROSS\_TITLE:  
CROSS\_TO:  
CUSTODIAN/SOURCE: Google  
DATECREATED: 12/15/2021  
DATELASTMOD: 12/15/2021  
DATERCVD:  
DATESENT:  
DeDuplicatedCustodians: Google  
DOEXT: DOCX  
FILENAME: Chrome\_Incognito\_NTP\_Revamp\_\_\_PRD.docx  
ILS\_ProdDate: 02/11/2022  
CROSS\_ILS\_ProdDate:  
MD5 HASH: B19CA554D51E64C98B13E7C48FA81246  
MessageID:  
NATIVEFILE:  
Owner:  
PAGES: 5  
REDACTED: Y  
SUBJECT:

# Mao Declaration

## Exhibit 25

Sealed Entirely

GOOG-CABR-05150754

# Mao Declaration

## Exhibit 26

Sealed Entirely

GOOG-BRWN-00166653

# Mao Declaration

## Exhibit 27

Sealed Entirely

GOOG-CABR-05145513

# Mao Declaration

## Exhibit 29

Redacted Version of Document  
Sought to Be Sealed

GOOG-BRWN-00388293



## Message

**From:** Mardini [mardini@google.com]  
**Sent:** 4/30/2019 7:14:16 PM  
**To:** Jochen Eisinger [eisinger@google.com]; Shimi Rahim [srahim@google.com]  
**CC:** Margret Schmidt [margrets@google.com]; Parisa Tabriz [parisa@google.com]; Alex Ainslie [ainslie@google.com]  
**Subject:** Re: Branding for Incognito (IO Update)

[narrowing down list of recipients - pls don't forward]

An update on our meeting with Sammit today. We discussed the following:

- 1/ Debugging the process
- 2/ Got context around the incognito iconography/rebranding for I/O then cancellation
- 3/ Got clarity on who owns that Incognito comms doc and whether our comments are being addressed

1/ Made it clear what the ideal process should be from Chrome's point of view. No disagreements there and it was clear for them but there was a mad rush to get things for I/O from various execs that made folks panic.

2/ This was driven by Lorraine who told the PDPO steering committee that Incognito might need rebranding so a workstream ensued involving the brand studio about 2-3 weeks ago.

Yesterday, at the PDPO SC meeting, Tom Oliveri was present and told them that Sundar didn't want to put incognito under the spotlight so this iconography/rebranding should not be an I/O topic.

The plan of record with regards to incognito in I/O is just to mention in one or two sentences related to bringing Incognito to Google Maps (not clear whether there will be mocks or not for that).

The SC was asked to commit to exploring in 2019 to develop a consistent vision for how an "Incognito 2.0" would look like with impact analysis on revenue, usage, and comms.

Relatedly, Ben Gomes showed a demo of AGSA launching Chrome in Incognito mode. i.e. if a user is in AGSA and they want to conduct an incognito search, they'd intent into an Incognito NTP in Clank

3/ That comms doc is owned by the brand studio and Sundar's speech writing team. I emphasized the need to double check with Chrome PM/Eng the accuracy of the information mentioned there. Sammit acknowledged but mentioned that the comms around I/O are very closely guarded and it's challenging to get a full picture for what will be said exactly....

Thanks,

--Mardini

On Tue, Apr 30, 2019 at 8:40 AM Mardini <mardini@google.com> wrote:

Le mar. 30 avr. 2019 à 08:33, Mardini <mardini@google.com> a écrit :

Thank you, Alex.

We (Rory/Ramin/Sabine/myself) have a meeting with Sammit today so will discuss the process and work cadence issue as well.

As discussed in our chat yesterday, Jochen and I will try to get some time with the PDPO folks visiting Munich for GSEC in a couple of weeks to sync in person.

I also didn't receive the note below about revisiting the incognito brand after I/O. Maybe it was sent only to those who replied "yes" to the meeting.

I see it now. Gmail didn't classify it as important :/.

Le mar. 30 avr. 2019 à 07:29, Yuan Chen <[yuanchen@google.com](mailto:yuanchen@google.com)> a écrit :

Thank you for keeping us in the loop - I also didn't get the update from PDPO. I agree we need to get into a better work cadence with PDPO folks.

On Tue, Apr 30, 2019 at 2:12 AM Shimi Rahim <[srahim@google.com](mailto:srahim@google.com)> wrote:

Thanks for filling us in, Alex & Parisa (I didn't see an email from PDPO), and for helping us navigate I/O challenges!

On Mon, Apr 29, 2019 at 5:03 PM Parisa Tabriz <[parisa@google.com](mailto:parisa@google.com)> wrote:

On Mon, Apr 29, 2019 at 4:42 PM Alex Ainslie <[ainslie@google.com](mailto:ainslie@google.com)> wrote:  
(narrowing to just Chrome folks)

I'm glad to see the update from PDPO below about waiting to tackle any branding updates until After IO.

Ah, me too!

Their timing was too aggressive and their proposal wasn't compelling :/

Here's the Chrome summary from my discussions with many of you (in sequence) this morning:

- Chrome is comfortable with a high level message at IO about expanding Incognito to other flagship Google products on Android (AGSA, Maps, YouTube).
- We've nurtured the Incognito brand for the past 10 years and our team would need to conduct a significant investigation (including UX Research) to feel confident about a change.
- For that reason, Chrome does not support announcing new PDPO-proposed branding at IO
- Additionally, speculative announcements related to Privacy are extra risky because the bar for Google is high and we need to make sure not to promise something we can't deliver.

#### Chrome + PDPO (Mis)alignment

Should Google ...	PDPO + Brand Studio	Chrome
... do more product work focused on Privacy?	Yes	Yes
... talk more about that Privacy work in public?	Yes	Yes
... extend Chrome's Incognito mode to other products?	Yes	Maybe?
... change the current Incognito brand?	Yes	Maybe? Err
... announce Incognito branding changes at IO before they've been thoroughly studied?	Yes	No

Going forward, I agree with Jochen that we'll need to get into a better working cadence with PDPO folks.

Yep. I'd recommend syncing with [miraglia@](mailto:miraglia@) in a small setting to share how this effort was perceived from the Chrome side so we can reset.

Alex

On Mon, Apr 29, 2019 at 4:00 PM Sammit Adhya <[sadhya@google.com](mailto:sadhya@google.com)> wrote:

Hi Everyone,

Just wanted to let you know that leads decided to revisit the Incognito branding after I/O. Apologies for scheduling the urgent meeting, but we look forward to working with everyone after I/O.

Thanks much,

Sammit

### **[Confirmed] - Exploration of Iconography and Branding for Incognito**

#### ***Scheduled per Sammit's request***

We wanted to share some new Incognito branding and iconography ideas that the Brand Studio team has been exploring to get your thoughts and feedback.

Leads: anilsa, parisa, miraglia

PM: (rorymccllland), (sabineb), mardini

Eng: eisinger, (rhalavati)

UXR: martinshelton, (lorindole)

UXD: ainslie

Marketing: martinal, jcroom

Brand: mediha, julianneyi, frederick

PDPO: sadhya, gregfair, rast

When Tue Apr 30, 2019 3:30pm – 4pm Pacific Time - Los Angeles

Where MTV-900-2-ChromeOZone (8) [GVC, No External Guests], MTV-900-2-Rage Against The Machine (4) [GVC, No External Guests], SFO-1MST-14-Daniel Handler (4) [GVC], SFO-2HS-4-Eight O'Clock Coffee (5) [GVC], SYD-ODI-3-410 - Gone (2) [GVC, No External Guests, Phone] ([map](#))

Joining info

[More phone numbers](#)

Who

- Eric Miraglia - organizer
- Jieun Lee - creator
- Martin Shelton
- Sammit Adhya
- [rast@google.com](mailto:rast@google.com)
- Martina Laresova
- Ken Frederick
- Jochen Eisinger
- James Croom
- Anil Sabharwal
- Mediha Abdulhay
- Greg Fair
- Alex Ainslie
- Shimi Rahim
- AbdelKarim Mardini
- Martha Welsh
- Julianne Yi
- Parisa Tabriz

- Ramin Halavati - optional
- Lorin Dole - optional
- Sabine Borsay - optional
- Rory McClelland - optional

--

**Yuan Chen**

Interaction Designer

Google Germany GmbH

Erika-Mann-Str. 33

80636 München

Geschäftsführer: Paul Menole, Hallimah DeLaine Prado  
Registernummer und -nummer, Hamburg, HRB 88881  
Sitz der Gesellschaft: Hamburg

Diese E-Mail ist vertraulich. Wenn Sie nicht der richtige Adressat sind, teilen Sie dies bitte nicht weiter, informieren Sie den Absender und löschen Sie die E-Mail und alle Anhänge. Vielen Dank.

This e-mail is confidential. If you are not the right addressee please do not forward it, please inform the sender, and please erase this e-mail including any attachments. Thanks.

PRODBEG: GOOG-BRWN-00388293  
PRODBEGATT:  
PRODEND: GOOG-BRWN-00388296  
PRODENDATT:  
PRODVOL: PROD028  
2nd\_CROSS\_BEGBATES:  
2nd\_CROSS\_ENDBATES:  
AllCustodians: AbdelKarim Mardini  
TO: jochen eisinger <eisinger@google.com>;shimi rahim <srahim@google.com>  
FROM: mardini <ardini@google.com>  
CC: parisa tabriz <parisa@google.com>;alex ainslie <ainslie@google.com>;margret  
schmidt <margrets@google.com>  
BCC:  
CONFIDENTIALITY: Confidential  
CROSS\_ALLCUSTODIANS: AbdelKarim Mardini  
CROSS\_ATTACHMENTNAME:  
CROSS\_BEGATTACH:  
CROSS\_BEGBATES: GOOG-CABR-00224709  
CROSS\_CC: parisa tabriz <parisa@google.com>;alex ainslie <ainslie@google.com>;ma-  
rgret schmidt <margrets@google.com>  
CROSS\_CONFIDENTIALITY: CONFIDENTIAL  
CROSS\_CUSTODIAN: AbdelKarim Mardini  
CROSS\_DATECREATED:  
CROSS\_DATEMOD: 04/30/2019  
CROSS\_DATERECEIVED: 04/30/2019  
CROSS\_DATESENT: 04/30/2019  
CROSS\_DE-DUPED CUSTODIANS: AbdelKarim Mardini  
CROSS\_ENDATTACH:  
CROSS\_ENDBATES: GOOG-CABR-00224712  
CROSS\_FILEEXTENSION: eml  
CROSS\_FILENAME:  
CROSS\_FROM: mardini <ardini@google.com>  
CROSS\_MD5 HASH: 1965D5D98ACCB9D49C7EBD0CFECB78E2  
CROSS\_MESSAGE ID: <CAGQY0Od-g=UK1G7bexQVsaig5aiu+i5wd4edce\_3x+VoeBtV8w@mail.gmai-  
l.com>  
CROSS\_OWNER: mardini  
CROSS\_PRODVAL: CROSS-PROD002  
CROSS\_REDACTED: N  
CROSS\_SUBJECT: Re: Branding for Incognito (IO Update)  
CROSS\_TITLE: Re: Branding for Incognito (IO Update)  
CROSS\_TO: jochen eisinger <eisinger@google.com>;shimi rahim <srahim@google.com>  
CUSTODIAN/SOURCE: AbdelKarim Mardini  
DATECREATED:  
DATELASTMOD: 04/30/2019  
DATERCVD:  
DATESENT:  
DeDupedCustodians:  
DOEXT:  
FILENAME:  
ILS\_ProdDate: 07/02/2021  
CROSS\_ILS\_ProdDate: 09/01/2021  
MD5 HASH: 1965D5D98ACCB9D49C7EBD0CFECB78E2  
MessageID:  
NATIVEFILE:  
Owner: mardini

PAGES:

REDACTED: N

SUBJECT: Re: Branding for Incognito (IO Update)

# Mao Declaration

## Exhibit 30

Redacted Version of Document  
Sought to Be Sealed

GOOG-CABR-00501220



## Message

**From:** Ramin Halavati [rhalavati@google.com]  
**Sent:** 8/8/2019 1:40:33 PM  
**To:** Sammit Adhya [sammit@google.com]  
**CC:** Florian Uunk [feuunk@google.com]; Sabine Borsay [sabineb@google.com]; Rory McClelland [rorymcclelland@google.com]; Greg Fair [gregfair@google.com]; Burton Rast [rast@google.com]  
**Subject:** Re: SinRastro / Chrome

Hi Sammit,

Thanks a lot for the explanation, I totally agree that presenting a simpler and more clear user story would be a user trust gain.

Let's continue the discussion on alternatives in the next week's meeting.

Best,  
 Ramin

On Thu, Aug 8, 2019 at 6:29 AM Sammit Adhya <[sammit@google.com](mailto:sammit@google.com)> wrote:

Hi Ramin,

Thanks for continuing to be so thoughtful about this. I definitely understand the risks of walking back on this narrative. At a high level, what we're really trying to address is the risk of a user who prefers to be private having their privacy actually eroded through data collection because we don't know of their intention to be private. Assuming we can solve the PR narrative, I believe that preventing the data collection is better for the user and we should be able to tell that story in a way that users understand.

To be perfectly clear, the data collected while Incognito is strictly **NOT** anonymous. When using a Google service, data (e.g. search queries) is tied to a pseudonymous ID (e.g. zwieback) that is then stored with the user's IP address, user agent, and other metadata (everything in the gwslog proto). While we don't connect it to a user's identity and there are many internal policies to ensure it does not happen, it's not impossible. Further, under the GDPR, data tied to unauthenticated identifiers **IS** considered to be personal data. [See GDPR analysis here](#). That means everything a user does while signed out of Google services is considered to be personal data.

In terms of users' perception, there are dozens of articles that discuss the fact that Incognito is not really all that private because of the data collected while using it, and some that point out that Google is still "tracking you". Here's a sample:

- [Google Denies Tracking People Through Incognito Mode - But Doesn't Say It's Not Possible](#)
- [Google Chrome's Incognito Mode is way less private than you think](#)
- [Google Chrome's Incognito Mode may not be as private as you think](#)
- [Chrome's anonymous browsing feature isn't as secret as we assumed](#)
- [Google denies claim that it's tracking internet users when incognito mode is on](#)
- [Why should I use DuckDuckGo while Google in Incognito does the same thing? \(Quora\)](#)

Realize that some of these are misconceptions and some are inaccurate, but that is kind of irrelevant. It's about the perception. Imagine being able to make the promise that if you use Google services while Incognito, we won't save your data. Period. That is an incredibly powerful statement for a company like Google to make. Of course, users may not understand some of these distinctions and maybe they won't understand the benefit, but I believe it is in their best interest.



Additionally, this battle of "detecting Incognito" seems like it will be never ending.. sounds like there is research attempting to work around the fix in 76 [method 1, method 2]. That's not to say these work, or we can't accomplish this, but we potentially might be continuously trying to stay ahead, while making privacy worse by collecting Incognito when the user has clearly told Chrome that it wants to be private. That is the fundamental reason for trying to strengthen Incognito and allow Google services to actually deliver on the promise of being private.

Let's continue chatting about the other concerns at our sync next week as well as next steps. Hopefully this helps levelset on the user benefit. I'm also trying to find some time with comms/PR/policy so we can walk through how we might approach that aspect.

Thanks again,  
Sammit

On Tue, Aug 6, 2019 at 5:47 AM Ramin Halavati <[rhalavati@google.com](mailto:rhalavati@google.com)> wrote:  
Hi Sammit,

[REDACTED]

[REDACTED]

3) Having the NTP solution as a just-in-time control might be hard, and if users are not opted in to 3rd party cookie blocking and have previously opened tabs, there might be leakage risks on changing this toggle's state. But this is something that we can work on the details and assess the risks and maybe warn user accordingly. But given that this is already a complicated issue to communicate to users, it seems safer to stay on the simpler side.

4) Sorry to jump back to this issue but I discussed the proposals today with Chrome privacy team and I think that to convince Chrome team about the letting-websites-know solution, we definitely need a good answer to the following two questions:

1. Why this is beneficial for the users and knowing that Google gets anonymous ids in incognito and they are no way connected to users' identities, how can we tell users that this is done for their benefit?
2. What would be the PR narrative that doesn't damage Chrome's user trust, when a few months ago we strongly defended private-browsing's anonymity and now we are changing the case.

I **strongly** believe that if we proceed to steering committee and even if they approve either of these letting-websites-know approaches, we would get the push back from Chrome team later, so it's better to work through these issues first and have an initial answer for them. This would be much more severe if we go towards a default-on approach where users just have the option to opt-out.

5) Can we have a more clear representation of regulator's requirement? Do they really care if Google stops logging anything in Chrome incognito mode or private browsing in general? Current approach is quite Chrome browser specific and if we won't have the feature as default-on (which requires item 4) the most we can get is an option for users to tell Google they don't want logging.

Thanks,

Ramin

P.S. Here are two articles defending keeping private-browsing hidden:

What Chrome's Incognito changes mean to the metered paywall vs. freemium debate  
Chrome 76 and the End of the Incognito Loophole

On Tue, Aug 6, 2019 at 4:22 AM Sammit Adhya <[sammit@google.com](mailto:sammit@google.com)> wrote:

Hi Ramin,

What would be the downside to blocking 3p cookies while Incognito?

Having a toggle on the NTP page as a "just-in-time" control that is only valid for the session is also interesting.

Thanks,  
Sammit

On Mon, Aug 5, 2019 at 3:57 AM Ramin Halavati <[rhalavati@google.com](mailto:rhalavati@google.com)> wrote:

Hi All,

What do you think?

Best,  
Ramin

On Mon, Aug 5, 2019 at 8:13 AM Sammit Adhya <[sammit@google.com](mailto:sammit@google.com)> wrote:

Hi All,

Just wanted to circle back here based on the conversation with Ramin last week.

I added a slide with some pros and cons so PTAL. Both seem like reasonable options so let's continue to get feedback. I'll also set up some time with our comms/policy folks to better understand what an option like this could mean and if there's a narrative that might work. Will include martinal@ in that conversation.

Thanks so much for the continued thoughtfulness on thinking through these proposals!

Best,  
Sammit

On Tue, Jul 30, 2019 at 6:25 AM Ramin Halavati <[rhalavati@google.com](mailto:rhalavati@google.com)> wrote:

Hi Sammit,

Thanks, let's continue the discussion in today's meeting. My general concern for the approach is:

- Since many websites may start adding this permission request, we need to add a way for users to dismiss spamming permission requests, which most probably would include an option to "Say no to all".
- Expecting that most users go with this easy option and don't fine tune it for different websites, I don't expect Google would also receive that much positive answer.
- Therefore, instead of the expected result of *"Going to incognito mode stops Google logging in all products"*, we would have *"Users have a way to set up Incognito to tell Google to stop logging for all products"*. This is not what Sundar promised.

Hence I see the solution mostly as a remedy for Google to tell regulators that we gave the option to the users, but they didn't use it, and not a feature for the users.

And if we really want to have a solution that gives the first promise, we should find a way to go through the PR issues of it and set this feature on-by-default, removing websites need to ask request to know, and provide users an approach to hide it from some/all websites.

Best,  
Ramin

On Mon, Jul 29, 2019 at 8:03 AM Sammit Adhya <[sammit@google.com](mailto:sammit@google.com)> wrote:  
+Steve Hamilton (PDPO UXR) as FYI

Hi Ramin,

Sorry for the delay! Answers inline below.

Thanks,  
Sammit

On Fri, Jul 26, 2019 at 1:05 AM Ramin Halavati <[rhalavati@google.com](mailto:rhalavati@google.com)> wrote:  
Hi,

And another question that popped up while working on the design spec of this proposal: What is the main problem that we want to solve with the new Sin Rastro proposal?

Is it just *"Google websites want to be able to distinguish new users from private-browsing users, so that they stop logging in private-browsing"*, or I am missing something?

If that's all, can we describe it as a user problem instead of Google problem and say what would be the benefit for users and to get what, would they say yes to a prompt to let the website know they are in private browsing?

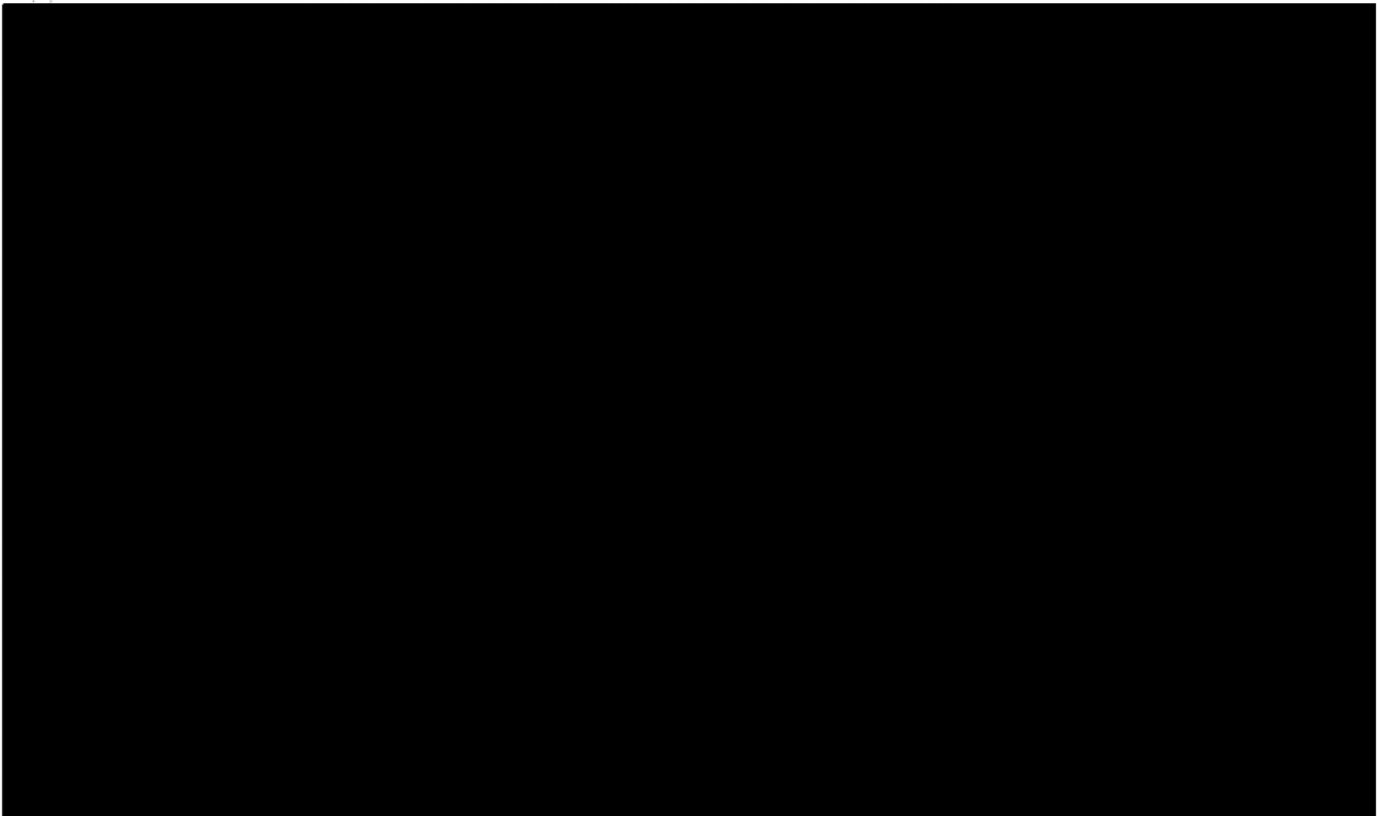
That's definitely one of the bigger problems we're trying to solve (largely because this is the space that we have direct control over).

>From an ecosystem perspective, do you think 3p websites would want to be more proactive when Incognito? Is there a world where we have a W3C spec that defines what it means for a website to support Incognito? If so, then the problem extends beyond just Google websites.

In the long-run, ideally, we move towards a world where we do this by default for signed out users. We'll be sure to highlight that being another option.

Thanks,  
Ramin

On Thu, Jul 25, 2019 at 12:53 PM Ramin Halavati <[rhalavati@google.com](mailto:rhalavati@google.com)> wrote:  
Hi,



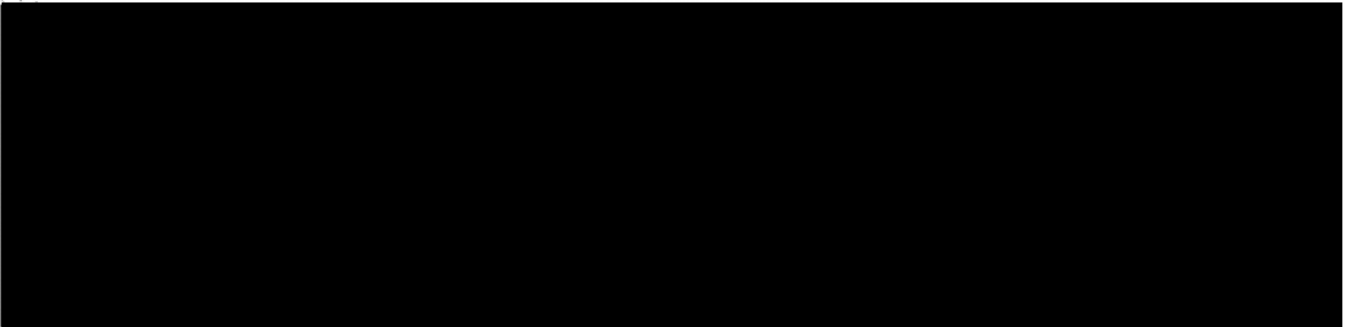
Thanks,  
Ramin

On Fri, Jul 19, 2019 at 4:12 PM Florian Uunk <[feuunk@google.com](mailto:feuunk@google.com)> wrote:

Thanks for the productive session! I took some super rough notes:

Proposed solution for telling the server to do Sin Rastro:

Websites publish that they offer incognito mode, user chooses whether they want to expose it.





Spaces overlap:

We'll work on notifications for any sign-in in incognito

When can we block sign-ins to Google? Need profile creation and usage in usable state first

What about incognito vs. Guest

We could make the default for incognito to not bring data.

Would be more aligned with native app incognito modes.

Would have to keep the functionality of bringing your data along, just moving it.

Proposal: do not bring data, and merge guest mode into incognito?

Could have a setting to bring in the data on the incognito NTP?

### SinRastro / Chrome

When Fri 19 Jul 2019 13:00 – 17:00 Central European Time - Berlin

Where MUC-ARP-3Z0-Seaview (8) [GVC] ([map](#))

Joining info

**Redacted - Privacy**

[More phone numbers](#)

Who

- Ramin Halavati- organiser
- Rory McClelland
- Sammit Adhya
- Greg Fair
- Florian Uunk - optional
- [rast@google.com](mailto:rast@google.com) - optional
- Sabine Borsay - optional

--

Sammit Adhya | Privacy and Data Protection | [sammit@google.com](mailto:sammit@google.com) | (650) 253-3001

--

Sammit Adhya | Privacy and Data Protection | [sammit@google.com](mailto:sammit@google.com) | (650) 253-3001

--

Sammit Adhya | Privacy and Data Protection | [sammit@google.com](mailto:sammit@google.com) | (650) 253-3001

--

Sammit Adhya | Privacy and Data Protection | [sammit@google.com](mailto:sammit@google.com) | (650) 253-3001

PRODBEG: GOOG-CALH-00452518  
PRODBEGATT:  
PRODEND: GOOG-CALH-00452524  
PRODENDATT:  
PRODVOL: CROSS-PROD002  
2nd\_CROSS\_BEGBATES:  
2nd\_CROSS\_ENDBATES:  
AllCustodians: Florian Uunk;Greg Fair  
TO: sammit adhya <sammit@google.com>  
FROM: ramin halavati <rhalavati@google.com>  
CC: sabine borsay <sabineb@google.com>;florian uunk <feuunk@google.com>;rory mcc-  
lelland <rorymcclelland@google.com>;burton rast <rast@google.com>-  
;greg fair <gregfair@google.com>  
BCC:  
CONFIDENTIALITY: CONFIDENTIAL  
CROSS\_ALLCUSTODIANS:  
CROSS\_ATTACHMENTNAME:  
CROSS\_BEGATTACH:  
CROSS\_BEGBATES: GOOG-CABR-00501220  
CROSS\_CC:  
CROSS\_CONFIDENTIALITY:  
CROSS\_CUSTODIAN:  
CROSS\_DATECREATED:  
CROSS\_DATEMOD:  
CROSS\_DATERECEIVED:  
CROSS\_DATESENT:  
CROSS\_DE-DUPED CUSTODIANS:  
CROSS\_ENDATTACH:  
CROSS\_ENDBATES: GOOG-CABR-00501226  
CROSS\_FILEEXTENSION:  
CROSS\_FILENAME:  
CROSS\_FROM:  
CROSS\_MD5 HASH:  
CROSS\_MESSAGE ID:  
CROSS\_OWNER:  
CROSS\_PRODVAL:  
CROSS\_REDACTED:  
CROSS\_SUBJECT:  
CROSS\_TITLE:  
CROSS\_TO:  
CUSTODIAN/SOURCE: Greg Fair  
DATECREATED:  
DATELASTMOD: 08/08/2019  
DATERCVD: 08/08/2019  
DATESENT: 08/08/2019  
DeDupedCustodians: Florian Uunk;Greg Fair  
DOEXT: eml  
FILENAME:  
ILS\_ProdDate: 09/01/2021  
CROSS\_ILS\_ProdDate: 09/01/2021  
MD5 HASH: D1DAF97F975FC8862D5BAD079BF2D73F  
MessageID: <CAORodQiMFEHGeoNcGg4JzhYqjfVKDSUsGNuk=qEAdM2uU5VD4Q@mail.gmail.com>  
NATIVEFILE:  
Owner: rhalavati  
PAGES: 7

REDACTED: Y

SUBJECT: Re: SinRastro / Chrome



# Mao Declaration

## Exhibit 31

Sealed Entirely

GOOG-BRWN-00428101

# Mao Declaration

## Exhibit 32

Sealed Entirely

GOOG-CABR-03849022

# Mao Declaration

## Exhibit 33

Sealed Entirely

GOOG-BRWN-00686207

# Mao Declaration

## Exhibit 36

Redacted Version of Document  
Sought to Be Sealed

GOOG-BRWN-00529122

Steve Hamilton &lt;sthamilton@google.com&gt;

**What we know about Incognito users (re. The most underused Privacy Surface)**

7 messages

Steve Hamilton &lt;sthamilton@google.com&gt;

Wed, Jan 27, 2021 at 1:41 PM

To: leathern@google.com, Othar Hansson <othar@google.com>, Mark Risher <risher@google.com>, Rahul Roy-Chowdhury <rahulrc@google.com>, Sarah Hammond <shammond@google.com>, Lauren Palmer <laurenpalmer@google.com>, Gretchen Gelke <ggelke@google.com>, Arne de Booij <adebooij@google.com>, Tal Herman <talherman@google.com>, Guemmy Kim <guemmy@google.com>, Kalle Buschmann <kallebu@google.com>

Hi Everyone,

I'm Steve, a UXR in the PDPO working on Sin Rastro (Google-wide Incognito mode).

Attached is a deck that summarizes what we know about Incognito users, what they use it for, and some of the risks that we've identified over the course of the project.

It's worth noting that the Chrome team have done some excellent work in this space (as you might expect), and are putting together some very interesting plans in go/incognito2021 (slides 24 to 31 are probably the most relevant)

Please feel free to reach-out with any questions or concerns, I'm more than happy to help.

Best,

Steve

TL;DR of the deck:

Executive Summary

- Frequency of Use:
  - Incognito mode is used by [REDACTED] of Chrome users, and [REDACTED] use it at least once per week
- User Characteristics:
  - Weekly users are more likely to be [REDACTED]  
[REDACTED] of weekly users state, [REDACTED] implying that they are more privacy sensitive than non-users, and may be more open to other privacy controls
- Top use cases for Incognito mode:  
[REDACTED]  
[REDACTED]
- Risks to press cycles on Incognito mode:
  - Users overestimate the protections that Incognito provides and are unaware of the personalization and data collection that occurs when it is on
  - When considered together, Incognito mode appears to negatively impact user sentiment towards regular browsing
  - Educational moments intended to reassure and inform users of quality-of-life features (autofill & autocomplete) have led to negative reactions

Rob Leathern &lt;leathern@google.com&gt;

Wed, Jan 27, 2021 at 3:47 PM

To: Steve Hamilton <sthamilton@google.com>, Annie Klemp <annieklemp@google.com>, Sam Heft-Luthy <heftluthy@google.com>, Ane Fabo Aranzabal <anefabo@google.com>  
 Cc: Othar Hansson <othar@google.com>, Mark Risher <risher@google.com>, Rahul Roy-Chowdhury <rahulrc@google.com>, Sarah Hammond <shammond@google.com>, Lauren Palmer <laurenpalmer@google.com>, Gretchen Gelke <ggelke@google.com>, Arne de Booij <adebooij@google.com>, Tal Herman <talherman@google.com>, Guemmy Kim <guemmy@google.com>, Kalle Buschmann <kallebu@google.com>

Thanks Steve, appreciate the update. Will let you know any questions as we dig into the data/insights.

@Annie Klemp / @Ane Fabo Aranzabal / @Sam Heft-Luthy for context.  
 Rob

[Quoted text hidden]

**Sarah Hammond** <shammond@google.com>  
 To: Steve Hamilton <sthamilton@google.com>

Wed, Jan 27, 2021 at 5:43 PM

Thanks so much, Steve!

[Quoted text hidden]

--

Sarah Hammond | UX Director, User and PDPO | shammond@google.com |  
 Sign up for my office hours: go/shammond-oh

**Steve Hamilton** <sthamilton@google.com>  
 To: Sarah Hammond <shammond@google.com>

Thu, Jan 28, 2021 at 8:25 AM

No worries, Sarah! I appreciate being asked to contribute :)

[Quoted text hidden]

**Othar Hansson** <othar@google.com>

Thu, Feb 4, 2021 at 5:16 PM

To: Rob Leathern <leathern@google.com>, Micha Segeritz <mseg@google.com>  
 Cc: Steve Hamilton <sthamilton@google.com>, Annie Klemp <annieklemp@google.com>, Sam Heft-Luthy <heftluthy@google.com>, Ane Fabo Aranzabal <anefabo@google.com>, Mark Risher <risher@google.com>, Rahul Roy-Chowdhury <rahulrc@google.com>, Sarah Hammond <shammond@google.com>, Lauren Palmer <laurenpalmer@google.com>, Gretchen Gelke <ggelke@google.com>, Arne de Booij <adebooij@google.com>, Tal Herman <talherman@google.com>, Guemmy Kim <guemmy@google.com>, Kalle Buschmann <kallebu@google.com>

+Micha Segeritz also

[Quoted text hidden]

**Micha Segeritz** <mseg@google.com>  
 Cc: Steve Hamilton <sthamilton@google.com>

Thu, Feb 4, 2021 at 6:34 PM

Hi Steve (just.you),

Where does this come from: Incognito mode is used by [REDACTED] of Chrome users, and [REDACTED] use it at least once per week (i don't have access.to the deck).

It's a lot higher than what I would have assumed based on inspecting the chrome client data.

Thanks,

Micha

[Quoted text hidden]

**Steve Hamilton** <sthamilton@google.com>

Fri, Feb 5, 2021 at 11:48 AM

To: Micha Segeritz <mseg@google.com>

Hi Micha,

You should have access to the summary deck now. The stats are self-reported from our Incognito survey. I agree, it does seem high given what Chrome report. I think it's a combination of self-report biases (mis-remembering/overestimating frequency of use) and the fact that Chrome use zweiback cookie age as the indicator of Incognito usage (this was their method last time I heard - they may have a new metric now). This may underestimate those who stay in Incognito forever and/or have very long Incognito sessions as they would be classified as signed-out users.

It does also seem to align with some of the work that Florian has done on Chrome - good discussion amongst them in this doc.

LMK if you want to chat more,

Steve

[Quoted text hidden]

PRODBEG: GOOG-BRWN-00529122  
PRODBEGATT:  
PRODEND: GOOG-BRWN-00529124  
PRODENDATT:  
PRODVOL: PROD042  
2nd\_CROSS\_BEGBATES:  
2nd\_CROSS\_ENDBATES:  
AllCustodians: Steve Hamilton  
TO:  
FROM:  
CC:  
BCC:  
CONFIDENTIALITY: Confidential  
CROSS\_ALLCUSTODIANS:  
CROSS\_ATTACHMENTNAME:  
CROSS\_BEGATTACH:  
CROSS\_BEGBATES:  
CROSS\_CC:  
CROSS\_CONFIDENTIALITY:  
CROSS\_CUSTODIAN:  
CROSS\_DATECREATED:  
CROSS\_DATEMOD:  
CROSS\_DATERECEIVED:  
CROSS\_DATESENT:  
CROSS\_DE-DUPED CUSTODIANS:  
CROSS\_ENDATTACH:  
CROSS\_ENDBATES:  
CROSS\_FILEEXTENSION:  
CROSS\_FILENAME:  
CROSS\_FROM:  
CROSS\_MD5 HASH:  
CROSS\_MESSAGE ID:  
CROSS\_OWNER:  
CROSS\_PRODVAL:  
CROSS\_REDACTED:  
CROSS\_SUBJECT:  
CROSS\_TITLE:  
CROSS\_TO:  
CUSTODIAN/SOURCE: Steve Hamilton  
DATECREATED: 04/20/2021  
DATELASTMOD: 04/20/2021  
DATERCVD:  
DATESENT:  
DeDupedCustodians:  
DOEXT:  
FILENAME: Google.com Mail - What we know about Incognito use\_1rKcaGefM0SYVPHRZSb-  
sTuuzcLaIBXARo.pdf  
ILS\_ProdDate: 10/05/2021  
CROSS\_ILS\_ProdDate:  
MD5 HASH: E88EC423F6858B0AB674B84551EADFCB  
MessageID:  
NATIVEFILE:  
Owner: sthamilton@google.com  
PAGES:  
REDACTED: N



SUBJECT:

# Mao Declaration

## Exhibit 37

Redacted Version of Document  
Sought to Be Sealed

GOOG-BRWN 00176477

## Message

**From:** Greg Fair [gregfair@google.com]  
**Sent:** 7/22/2020 7:41:15 PM  
**To:** Sammit Adhya [sadhya@google.com]

- **Greg Fair**, 2020-07-22 12:41:15

What is this apas meeting later this afternoon and do I need to be there for you?

- **Greg Fair**, 2020-07-22 12:41:23

(To represent you)

- **Sammit Adhya**, 2020-07-22 13:59:30

Its thinking about the timeline required to get an iOS consent screen in time for iOS 14 launch

- **Sammit Adhya**, 2020-07-22 13:59:45

dan/virginia will be there

- **Sammit Adhya**, 2020-07-22 13:59:54

i think for me, i'm worried about bandwidth

- **Sammit Adhya**, 2020-07-22 14:00:35

i dont think virginia has a good sense of how to protect our time yet because we don't know the priorities

- **Greg Fair**, 2020-07-22 14:00:46

Why do we want that?

- **Greg Fair**, 2020-07-22 14:00:53

The iOS consent screen

- **Sammit Adhya**, 2020-07-22 14:00:58

IDFA ☺

- **Greg Fair**, 2020-07-22 14:01:27

Oh this is the thing that YT doesn't want?

- **Greg Fair**, 2020-07-22 14:01:59

NM. I will get my head straight.

- **Greg Fair**, 2020-07-22 14:02:14

(Obviously I think this is a lower priority)

- **Sammit Adhya**, 2020-07-22 14:02:38

this is to figure out what to do for iOS 14 launch in EEA and YT

- **Sammit Adhya**, 2020-07-22 14:02:40

sorry, wasnt clear

- **Sammit Adhya**, 2020-07-22 14:03:34

to get IDFA consent (and when)

- **Greg Fair**, 2020-07-22 14:04:05

Ah. I thought i read in that deck that they weren't going to do it.

- **Sammit Adhya**, 2020-07-22 14:04:16

oh i hadnt heard that

- **Greg Fair**, 2020-07-22 14:07:01

Slide 9 ?<br><br>The "Google wants to track you" message will have too much negative impact on user trust. iGA will not add the consent, but will monitor the iOS 14 rollout's impact to revenue.

- **Sammit Adhya**, 2020-07-22 14:07:14

yes IGA is not

- **Sammit Adhya**, 2020-07-22 14:07:19

YT will need to do something

- **Greg Fair**, 2020-07-22 14:07:56

oooooooooh. This is YT. Not iGA.

- **Sammit Adhya**, 2020-07-22 14:20:14

Yes sir

- **Greg Fair**, 2020-07-22 14:22:03

Sorry i didn't look at names carefully enough

- **Sammit Adhya**, 2020-07-22 14:33:55

Just got an email from Christina though that they are reconsidering

- **Sammit Adhya**, 2020-07-22 14:34:02

Impact is bigger than expected

- **Greg Fair**, 2020-07-22 14:41:58

Dumb question: why wouldn't we just let them figure it out on their own? And then do our own thing for unauth (or auth) later as planned?

- **Greg Fair**, 2020-07-22 14:42:29

Because consent rates are better if we do all at once?

- **Sammit Adhya**, 2020-07-22 14:44:26

i think its a question about what [REDACTED] is.. if our goal is a unified consent framework, then letting them do it on their own won't lead to that. We'll have different consent flows between iOS YT, IGA, web (and funding choices in theory)

- **Sammit Adhya**, 2020-07-22 14:44:55

i dont think its about consent rates.. though i imagine we're probably the most knowledgeable and have the most experience

- **Greg Fair**, 2020-07-22 14:45:40

Because this would be the same as the full epd consent? Plus idfa?

- **Sammit Adhya**, 2020-07-22 14:46:19

it could be.. that also begs the scope of scope, and how careful we want to be re: perception in EU

- **Sammit Adhya**, 2020-07-22 14:46:26

(sorry, so many caveats)

- **Sammit Adhya**, 2020-07-22 14:46:40

if we let them do it.. maybe they only build a warm up screen to get IDFA consent

- **Greg Fair**, 2020-07-22 14:46:40

Right.

- **Greg Fair**, 2020 07 22 14:46:46

Exactly.

- **Greg Fair**, 2020 07 22 14:46:49

Ok thanks.

- **Greg Fair**, 2020 07 22 14:46:57

I will attend the meeting. Thanks.

- **Greg Fair**, 2020 07 22 14:47:02

Sorry to bother you.

- **Sammit Adhya**, 2020 07 22 14:47:06

okay, appreciate it.. not at all

- **Sammit Adhya**, 2020 07 22 14:47:09

asha is sleeping

- **Sammit Adhya**, 2020 07 22 14:47:21

if by some mircle she has a long nap, will try to join

- **Sammit Adhya**, 2020 07 22 14:47:44

but we probably need to priortize to help our team.. i am def feeling stretched 😊

- **Sammit Adhya**, 2020 07 22 14:47:53

this is something we could technically carve out

- **Sammit Adhya**, 2020 07 22 14:47:58

mobile app consent

- **Greg Fair**, 2020 07 22 14:50:45

Yea that was my gut for sure

- **Sammit Adhya**, 2020 07 22 14:51:03

our eng team wont own it anyway

- **Greg Fair**, 2020 07 22 14:51:05

Or co-opt some folks into iOS ■

- **Greg Fair**, 2020 07 22 14:51:26

Maybe Jonathan or Sam ;)

- **Greg Fair**, 2020 07 22 14:51:50

Or Karen. Ha

- **Sammit Adhya**, 2020 07 22 14:52:07

ya jonathan has YT + consent experience so that would be amazing

- **Sammit Adhya**, 2020 07 22 14:52:11

it doesnt care about ads

- **Sammit Adhya**, 2020 07 22 14:52:11

lol

- **Sammit Adhya**, 2020 07 22 14:52:33

but he cares about yt watch/search history

- **Greg Fair**, 2020-07-22 14:52:39

Right.

- **Sammit Adhya**, 2020-07-22 14:53:25

hah, karen.. that would be fun to watch

- **Sammit Adhya**, 2020-07-22 14:54:16

also, we have to talk about this search detecting Incognito thing! am i overindexing?

- **Sammit Adhya**, 2020-07-22 14:55:13

on one hand.. its like, great! We know already!! Let's not show consent using that.. LOL. on the other.. yikes, doubled down on a promise we don't keep.

- **Greg Fair**, 2020-07-22 14:56:08

Since it is clear it has been there for a while this doesn't seem like our problem to solve immediately. (Esp because we want this to happen in some way anyway)

- **Greg Fair**, 2020-07-22 14:56:15

If anything it's an opportunity.

- **Greg Fair**, 2020-07-22 14:56:19

Let's do it right!

- **Sammit Adhya**, 2020-07-22 14:56:51

ya the chrome team will escalate very quickly if they get wind of it..

- **Greg Fair**, 2020-07-22 14:58:18

If they cared that much this wouldn't exist in the first place.

- **Greg Fair**, 2020-07-22 14:58:42

(Maybe he is wrong btw)

- **Sammit Adhya**, 2020-07-22 14:59:35

yeah true

- **Sammit Adhya**, 2020-07-22 14:59:52

okay well let's strategize next time we talk about how we can do things with this loophole :)

- **Sammit Adhya**, 2020-07-22 14:59:55

thanks

- **Greg Fair**, 2020-07-22 15:52:28

just fyi cuz interesting (from meeting)<br>here is the top-level [REDACTED]: <a href="https://www.google.com/url?q=https://experiments.corp.google.com/%23/portal/experiments/analysis?label%3D\_%3D:cTWUD0OpbAQftvVnSbGwTC\_txVA&sa=D&source=hangouts&ust=1595544748544000&usg=AFQjCNFgxtMOz0tGsrHVI7qF4FFDJVzj7Q">https://experiments.corp.google.com/#/portal/experiments/analysis?label=\_:cTWUD0OpbAQftvVnSbGwTC\_txVA</a><br>[REDACTED] of IOS revenue comes from signed-out<br>and EU is [REDACTED] of the IOS signed-out queries<br>Fatih Boyaci3:45 PM<br>EU (including GB/UK)<br>Fatih Boyaci3:47 PM<br>so if we do basic math EU-IOS-Signed-out will be [REDACTED] (w/ EU CPMs being higher we can say [REDACTED] of covered rev)



PRODBEG: GOOG-BRWN-00176477  
PRODBEGATT:  
PRODEND: GOOG-BRWN-00176480  
PRODENDATT:  
PRODVOL: PROD023  
2nd\_CROSS\_BEGBATES:  
2nd\_CROSS\_ENDBATES:  
AllCustodians: Greg Fair  
TO: sammit adhya <sadhya@google.com>  
FROM: greg fair <gregfair@google.com>  
CC:  
BCC:  
CONFIDENTIALITY: Highly Confidential - AEO  
CROSS\_ALLCUSTODIANS: Greg Fair  
CROSS\_ATTACHMENTNAME:  
CROSS\_BEGATTACH:  
CROSS\_BEGBATES: GOOG-CABR-00190452  
CROSS\_CC:  
CROSS\_CONFIDENTIALITY: HIGHLY CONFIDENTIAL - ATTORNEYS' EYES ONLY  
CROSS\_CUSTODIAN: Greg Fair  
CROSS\_DATECREATED:  
CROSS\_DATEMOD: 07/22/2020  
CROSS\_DATERECEIVED: 07/22/2020  
CROSS\_DATESENT: 07/22/2020  
CROSS\_DE-DUPED CUSTODIANS: Greg Fair  
CROSS\_ENDATTACH:  
CROSS\_ENDBATES: GOOG-CABR-00190455  
CROSS\_FILEEXTENSION: eml  
CROSS\_FILENAME:  
CROSS\_FROM: greg fair <gregfair@google.com>  
CROSS\_MD5 HASH: 63640A782EDA5EE38A9528B34361CA58  
CROSS\_MESSAGE ID: <aljncaddtl6irq1adonaqbj8tqnemhk85gk2gi1c5jk4tj36gq0\_71o6ukqv-6984ujaeessk4kb9atqmaui7al2g\_chat@gmail.com>  
CROSS\_OWNER: gregfair  
CROSS\_PRODVAL: CROSS-PROD002  
CROSS\_REDACTED: N  
CROSS\_SUBJECT:  
CROSS\_TITLE: Outlook Express Mail Message  
CROSS\_TO: sammit adhya <sadhya@google.com>  
CUSTODIAN/SOURCE: Greg Fair  
DATECREATED:  
DATELASTMOD: 07/22/2020  
DATERCVD:  
DATESENT:  
DeDupedCustodians:  
DOEXT:  
FILENAME:  
ILS\_ProdDate: 06/18/2021  
CROSS\_ILS\_ProdDate: 09/01/2021  
MD5 HASH: 63640A782EDA5EE38A9528B34361CA58  
MessageID:  
NATIVEFILE:  
Owner: gregfair  
PAGES:  
REDACTED: N

SUBJECT:



# Mao Declaration

## Exhibit 38

Sealed Entirely

GOOG-CABR-00411915

# Mao Declaration

## Exhibit 39

Sealed Entirely

GOOG-BRWN-00067645

# Mao Declaration

## Exhibit 44

Redacted Version of  
Document Sought to Be Sealed

GOOG-CABR-05371009

## Message

**From:** Michael Kleber [kleber@google.com]  
**Sent:** 11/5/2018 7:36:49 PM  
**To:** Chris Palmer [palmer@google.com]  
**CC:** Mike West [mkwst@google.com]; [REDACTED]@google.com; chrome-privacy-core@google.com  
**Subject:** Re: EFF: "Google Chrome's Users Take a Back Seat to Its Bottom Line"

Thanks, Chris, that does help.

Much as I love the "We should continue to reach out and offer to help inform them" point of view in general, I don't think we're willing to tell anyone external that dropping 3p cookies from display ad requests costs sites half of their revenue. Even internally we hedge and point out that it's different for every site, which is true, but frankly I think this is so locked-down because we don't want to cause industry-wide panic.

Unfortunately, so long as we're unwilling to talk about this detail externally, I don't see a path to substantially changing the narrative.

—Michael

On Mon, Nov 5, 2018 at 2:16 PM Chris Palmer <palmer@google.com> wrote:

I have worked at EFF twice, first as Staff Technologist & Technology Manager, and again as Technology Director. So maybe I can provide some context. I left EFF and came to Google on the informed belief that I can successfully do more EFF-like work here than at EFF. After 7 years here, I am certain I was right. But, do take this with a grain of salt — I have A Viewpoint and it might not be 100% objective. :)

To answer Michael's question: It's ignorance, not malice. (Sure, they're feisty, but that is good!) Generally, EFF does not think hard about how people who create information goods make money. They have an old-timey Wired Magazine/1990s internet boom/techno-solutionist/"we're already post-scarcity!" ideology that requires them to believe that low marginal cost per copy means that information goods are 'free' to make. You'll see this in their positions on any information good, whether it's software, [music](#), journalism, literature, et c. (They rely heavily on [Cory Doctorow's hard-to-replicate experience of getting lucky](#), which notably involved running a popular ad-supported blog. Doot-de-doo...)

As for "credulous and naive", yes; part of their problem is epistemic closure. (Again, *not malice* — they are good people trying to do the right thing.) They tend to alienate people who could inform them, leaving only people who already agree. For example, they didn't ask me if they had the facts right before posting this post, despite knowing me and that I am on Chrome Security; similarly, AFAIK they have never had anyone who has ever been in the intelligence community on staff.

Their closure also reduces their potential reach, although they do have vocal support in parts of the security engineering community (and, weirdly, vocal opposition in other parts of the security community). We should continue to reach out and offer to help inform them. I don't necessarily expect huge returns from that; Google gave EFF an early view of Gmail and EFF still blasted them for its "creepiness", but I think it was good for everyone to at least have the conversation. It's better than random broadsides like this post.

Ultimately, the blame for people's misconceptions about Incognito Mode is due to that name and branding, as I have argued repeatedly. I believe the Incognito part of this blog post would basically not exist if we had called it (e.g.) Temporary Mode.



Could Incognito/Temporary work better, such as the site- or origin-specific local storage deletion? Sure, maybe that would work. As much as I want to ratchet down the brand and apparent 'guarantee', I am also in favor of ratcheting up the guarantee *where technically possible*. (I'll continue to push back on infeasible or impossible guarantees.)

On Mon, Nov 5, 2018 at 6:26 AM Michael Kleber <[kleber@google.com](mailto:kleber@google.com)> wrote:

I am really surprised by their never touching on how publishers get money. They (wrongly) claim that "The marginal benefit of each additional bit of information about your activities online is relatively small to an advertiser, especially given how much you directly give Google through your searches". But there is no corresponding thinking about the marginal benefit of the cookie is *huge for publishers*, because without it we have no way to bring *any* of that information to bear on display ad monetization.

Any opinion on whether that omission is ignorance or malice?

Their take on "incognito mode" is very interesting. The idea that it "does nothing to protect you from being tracked by Google" is a rational complaint if you sign into Google in incognito mode (which seems like an oxymoron to me), or if you use the same incognito session for a long time.

Have we considered an incognito mode which wipes storage on a site-by-site level? That is, as soon as you close your last tab from [foo.com](http://foo.com), all [foo.com](http://foo.com) storage is cleared? That doesn't quite get rid of 3p cookies, in that if you had incognito windows open from multiple domains at the same time, then one could get 3p cookies from the other. But it goes much farther in the "private browsing" direction that EFF is describing.

"A sustainable Web needs to be built on consent, not subterfuge" surprises me, in that I would have expected them to be as skeptical of consent as we are. Maybe political considerations mean you can't say that publicly (yet)?

--Michael

On Mon, Nov 5, 2018 at 3:27 AM Mike West <[mkwst@google.com](mailto:mkwst@google.com)> wrote:

Ouch. <https://www.eff.org/deeplinks/2018/11/google-chromes-users-take-back-seat-its-bottom-line>

A few things to call out:

"The closest thing it offers to 'private' browsing out-of-the-box is 'incognito mode', which only hides what you do from others who use your machine. That might hide embarrassing searches from your family, but does nothing to protect you from being tracked by Google." which is an interesting form of the "Incognito should do more" argument.

"Facebook recently announced its intention to [move away from using third-party cookies](#) to power Pixel, its third-party analytics product." is a fairly naive and credulous take on Facebook's moves in this space.

"Google could take the lead on solving this problem. Trackers are not necessary to make the Web work, and they shouldn't be necessary for Google to make lots (and lots) of money. As we noted above, Google has mountains of direct information about what you want to buy through its various services, from search to Maps to Google Play. Ads don't need to be targeted using every little bit of information about us that Google has access to via our use of its browser. A sustainable Web needs to be built on consent, not subterfuge." Apparently first-party tracking is fine.

"Google has come under fire in the past for using its power in one arena, like browsing or search, to drive revenue to other parts of its business." I heard a similar kind of argument from one of our friends at Samsung at dinner during TPAC a week or two ago.

-mike

--

You received this message because you are subscribed to the Google Groups "[REDACTED]" group.

To unsubscribe from this group and stop receiving emails from it, send an email to

[REDACTED][\[REDACTED\]unsubscribe@google.com](mailto:[REDACTED]unsubscribe@google.com).

To post to this group, send email to [REDACTED][@google.com](mailto:[REDACTED]@google.com).

To view this discussion on the web visit

[https://groups.google.com/a/google.com/d/msgid/\[REDACTED\]/CAKXHy%3Dc1Ovb%3DLbdoQeAa7r%2B9y2Kaya7G7xfmtZ3SzKKq8rOa%2BA%40mail.gmail.com](https://groups.google.com/a/google.com/d/msgid/[REDACTED]/CAKXHy%3Dc1Ovb%3DLbdoQeAa7r%2B9y2Kaya7G7xfmtZ3SzKKq8rOa%2BA%40mail.gmail.com).

--

Forewarned is worth an octopus in the bush.

--

You received this message because you are subscribed to the Google Groups "[REDACTED]" group.

To unsubscribe from this group and stop receiving emails from it, send an email to

[REDACTED][\[REDACTED\]unsubscribe@google.com](mailto:[REDACTED]unsubscribe@google.com).

To post to this group, send email to [REDACTED][@google.com](mailto:[REDACTED]@google.com).

To view this discussion on the web visit

[https://groups.google.com/a/google.com/d/msgid/\[REDACTED\]/CAA6DcCePf9riuRtP%3DgO0u4RUcG6A3%2Bi%3D4YCT2tPonpAPtW0VNg%40mail.gmail.com](https://groups.google.com/a/google.com/d/msgid/[REDACTED]/CAA6DcCePf9riuRtP%3DgO0u4RUcG6A3%2Bi%3D4YCT2tPonpAPtW0VNg%40mail.gmail.com).

--

Forewarned is worth an octopus in the bush.

--

You received this message because you are subscribed to the Google Groups "[REDACTED]" group.

To unsubscribe from this group and stop receiving emails from it, send an email to

[REDACTED][\[REDACTED\]unsubscribe@google.com](mailto:[REDACTED]unsubscribe@google.com).

To post to this group, send email to [REDACTED][@google.com](mailto:[REDACTED]@google.com).

To view this discussion on the web visit

[https://groups.google.com/a/google.com/d/msgid/\[REDACTED\]/CAA6DcCdpq3SfjVdc7yLTZBJ7EnecZWk2XM2DnYm0rtOK718p2A%40mail.gmail.com](https://groups.google.com/a/google.com/d/msgid/[REDACTED]/CAA6DcCdpq3SfjVdc7yLTZBJ7EnecZWk2XM2DnYm0rtOK718p2A%40mail.gmail.com).

PRODBEG: GOOG-CABR-05371009  
PRODBEGATT:  
PRODEND: GOOG-CABR-05371011  
PRODENDATT:  
PRODVOL: CROSS-PROD052  
2nd\_CROSS\_BEGBATES:  
2nd\_CROSS\_ENDBATES:  
AllCustodians: Adrienne Porter Felt;Chetna Bindra  
TO: chris palmer <palmer@google.com>  
FROM: michael kleber <kleber@google.com>  
CC: chrome-privacy-core@google.com [REDACTED]@google.com;mike west <mkwst@google.-com>  
BCC:  
CONFIDENTIALITY: HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY  
CROSS\_ALLCUSTODIANS:  
CROSS\_ATTACHMENTNAME:  
CROSS\_BEGATTACH:  
CROSS\_BEGBATES:  
CROSS\_CC:  
CROSS\_CONFIDENTIALITY:  
CROSS\_CUSTODIAN:  
CROSS\_DATECREATED:  
CROSS\_DATEMOD:  
CROSS\_DATERECEIVED:  
CROSS\_DATESENT:  
CROSS\_DE-DUPED CUSTODIANS:  
CROSS\_ENDATTACH:  
CROSS\_ENDBATES:  
CROSS\_FILEEXTENSION:  
CROSS\_FILENAME:  
CROSS\_FROM:  
CROSS\_MD5 HASH:  
CROSS\_MESSAGE ID:  
CROSS\_OWNER:  
CROSS\_PRODVAL:  
CROSS\_REDACTED:  
CROSS\_SUBJECT:  
CROSS\_TITLE:  
CROSS\_TO:  
CUSTODIAN/SOURCE: Adrienne Porter Felt  
DATECREATED:  
DATELASTMOD: 11/05/2018  
DATERCVD: 11/05/2018  
DATESENT: 11/05/2018  
DeDupedCustodians: Adrienne Porter Felt;Chetna Bindra  
DOEXT: eml  
FILENAME:  
ILS\_ProdDate: 12/02/2021  
CROSS\_ILS\_ProdDate:  
MD5 HASH: 171749A8C4DFF81D85D7D3992C4B279A  
MessageID: <CAA6DcCdpq3SfjVdc7yLTZBJ7EnecZWk2XM2DnYm0rtOK718p2A@mail.gmail.com>  
NATIVEFILE:  
Owner: kleber  
PAGES: 3  
REDACTED: N

SUBJECT: Re: EFF: "Google Chrome's Users Take a Back Seat to Its Bottom Line"



# Mao Declaration

## Exhibit 46

Redacted Version of Document

Sought to be Sealed

GOOG-BRWN-00047390

# Incognito Mode, Current and Possible Promises

Author: rhalavati@

Status: WIP

Last Update: 2018-09-24

[go/incognito\\_promises](#)

Please see [go/incognito-mode](#) for the updated incognito definition.

## Table of Contents

<b>Incognito Mode, Current and Possible Promises</b>	<b>1</b>
<b>Table of Contents</b>	<b>1</b>
<b>Intro</b>	<b>2</b>
<b>Chrome Promises</b>	<b>2</b>
Ephemeral State	3
User profile state should not change in incognito	3
No automatic scarification of privacy	3
Explicit warnings when privacy can't be guaranteed	3
Incognito mode and regular mode should not be linkable	4
Incognito mode should not be detectable	4
Default behavior of all features should respect incognito promises when called from incognito.	4
Enterprise Mode	4
<b>User Expectations</b>	<b>5</b>
Hide browsing history, especially visits to adult websites	5
Prevent targeted ads and search suggestions	5
Achieve "safer" browsing	5
Prevent browsers from saving login-related information	5
Avoid Cookies	6
Accommodate intentional or unintentional use by others.	6
Surfing Web Anonymously	6

Encrypted Communication with Websites	6
Hiding IP Address	6
<b>Future Possibilities</b>	<b>7</b>
[REDACTED]	7
[REDACTED]	7
[REDACTED]	7
[REDACTED]	7
[REDACTED]	7
[REDACTED]	8
[REDACTED]	8
<b>Possible plans for future</b>	<b>8</b>
[REDACTED]	8
[REDACTED]	9

## Intro

This document discusses the current promises of incognito mode, user's expectations and understanding of them, and the ways to improve.

Related docs: [go/incognito-mode](#), [go/incognito-prd/](#)

## Chrome Promises

As stated in incognito NTP, here are the general promises for incognito mode:

1. Chrome won't save your browsing history.
2. Chrome won't save your cookies and site data.
3. Chrome won't save your information entered in forms.

And it warns that the activity would still be visible to:

1. Websites<sup>1</sup>.
2. Employer or school.
3. Internet service provider.

Internally we are trying to keep the following extended list of promises.

---

<sup>1</sup> But does not say the websites that talk to the websites that you navigate (3rd parties).

## Ephemeral State

Unless there is a direct and clear user request, nothing should be stored on disk and if it is needed to do so, it should be encrypted while the key is kept in memory, and the data should be wiped on incognito mode close or next restart (in case of crash).

Downloads and saved files are examples of data that are stored by direct user action, browsing state in Android is a sample of encrypted on disk. Cookies have a separate jar that is cleared when incognito mode is closed.

## User profile state should not change in incognito

No change in user preferences in incognito mode should affect regular mode. Exceptions of this rule are accessibility features, and bookmarks.

## No automatic scarification of privacy

Any feature that disrespects privacy for a gain, should not be automatic in incognito and should be gated behind direct user action. Examples include:

- Autofill on incognito is not automatic and user needs selection of the suggested input to enter it.
- UKMs are disabled in incognito to avoid automatic data collection.
- Device identifiers or feature queries are completely behind user consent.
- All permissions are reduced towards factory default in incognito.
- Passing user information to other softwares is gated behind user consent or reduced. Whenever possible, passing user information to OS should also be restricted in incognito. For example, notifications through OS UI should be stripped from user data in incognito as they might be logged by the OS.

## Explicit warnings when privacy can't be guaranteed

Features that will affect the privacy of incognito mode should come with a clear warning, such as enabling extensions in incognito.

## Incognito mode and regular mode should not be linkable

Any signature that can be used to connect the user's regular and incognito mode browsing should be avoided. This is to some extent violated by fingerprinting.

## Incognito mode should not be detectable

We should not provide means for the websites to detect if the user is browsing in regular mode or incognito. To do so, all enabled features in incognito mode should seem similar to regular mode from a web facing point of view, and all disabled features, should be done so that it is done by the user. This is to some extent violated due to the missing features in incognito.

## Default behavior of all features should respect incognito promises when called from incognito.

Privacy sensitive features should be implemented to respect incognito promises when run from incognito mode, and overriding them should need direct specification. E.g., preferences are saved in memory in incognito mode by default, and exceptional cases that need in profile storage are white listed to do so.

## Enterprise Mode

Incognito mode should respect all the enforced policies. It would be good if Enterprise users would be warned that all specified policies are applied to the incognito mode as well and the promises are held in that context.

**Comment [1]:** +tnagel@google.com  
Do we have any specific Enterprise promises?

**Comment [2]:** Afaiu the basic promise is that "enterprise policies don't apply" (e.g. extensions), but I'm not sure whether thats codified somewhere.

**Comment [3]:** I updated the text, please take a look.

**Comment [4]:** +mnissler@google.com Hey Mattias, do you have strong feelings about this? -- I'm not sure whether I do.

**Comment [5]:** This is tricky. Force-installed extension don't get access to incognito by default IIRC. All policy controls that are browser-global and not specific to a profile will affect incognito. Thus, I don't think there's a single valid policy on how enterprise management behaves for incognito, it's always been case-by-case decisions.

For Chrome OS, I don't feel too strongly - the OS user account is managed, so it's not surprising that incognito sessions within that user are subject to (some) management. On top of that, we have guest sessions as our solution for people who want an ephemeral browsing session with more guarantees.

On desktop, the situation is pretty complicated. If you're on a corp machine, it's similar to Chrome OS. What about BYOD though? With a corp-managed Chrome profile? I honestly don't know what the correct behavior for that case would be...

## User Expectations

Based on Wu, et al.<sup>2</sup>, and Habib et al.<sup>3</sup>, users use private browsing for the following expectations.

<sup>2</sup> "Your Secrets Are Safe: How Browsers' Explanations Impact Misconceptions About Private Browsing Mode", Wu et al., Proceedings of the 2018 World Wide Web Conference.

<sup>3</sup> "Away From Prying Eyes: Analyzing Usage and Understanding of Private Browsing", Habib et al., Proceedings of the 14th Symposium on Usable Privacy and Security, Aug 2018, Baltimore, US.

## Hide browsing history, especially visits to adult websites

If we consider hiding browsing history local, Incognito is completely doing that by clearing it after closing the current session. If it would be considered from network (ISP), or school, employer, etc., incognito is not doing so, and clearly has stated that it is not doing so.

## Prevent targeted ads and search suggestions

This is done in incognito by separating the cookie jar and history in regular and incognito mode. We can consider it satisfied, but if a user stays long enough incognito mode and develop a new profile in incognito, this is not done.

## Achieve “safer” browsing

Incognito mode is about privacy and not security. Not in the promises and not fulfilled.

## Prevent browsers from saving login-related information

Similar to targeted ads, this is completely done by separating the cookie jars, but not in one incognito session.

## Avoid Cookies

Like above item. Maybe we should know why users want cookieless browsing. Does that mean 3rd party cookies and avoiding targeted ads, or some other functionality is desired.

## Accommodate intentional or unintentional use by others.

Partly done by not altering user profile or history in incognito mode, but better to be done in guest mode.

## Surfing Web Anonymously

Anonymous surfing is partly done by creating a fresh profile on each entry of the incognito mode. But fingerprinting to some extent disrupts the total clean slate, and maybe, users expect no trace from an inside one incognito session experience, which can be a cookie-siloed browsing.

## Encrypted Communication with Websites

Incognito mode does not enforce HTTPS, or even upgrade by default if it's safe.

## Hiding IP Address

Not covered.

## Future Possibilities

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]



## Possible plans for future

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

PRODBEG: GOOG-BRWN-00047390  
PRODBEGATT:  
PRODEND: GOOG-BRWN-00047398  
PRODENDATT:  
PRODVOL: PROD013  
2nd\_CROSS\_BEGBATES:  
2nd\_CROSS\_ENDBATES:  
AllCustodians: Helen Harris  
TO:  
FROM:  
CC:  
BCC:  
CONFIDENTIALITY: Confidential  
CROSS\_ALLCUSTODIANS: Helen Harris  
CROSS\_ATTACHMENTNAME:  
CROSS\_BEGATTACH:  
CROSS\_BEGBATES: GOOG-CABR-00704179  
CROSS\_CC:  
CROSS\_CONFIDENTIALITY: CONFIDENTIAL  
CROSS\_CUSTODIAN: Helen Harris  
CROSS\_DATECREATED: 07/31/2018  
CROSS\_DATEMOD: 12/14/2018  
CROSS\_DATERECEIVED:  
CROSS\_DATESENT:  
CROSS\_DE-DUPED CUSTODIANS: Helen Harris  
CROSS\_ENDATTACH:  
CROSS\_ENDBATES: GOOG-CABR-00704187  
CROSS\_FILEEXTENSION: docx  
CROSS\_FILENAME: 1- Incognito Mode Current and Possible\_1j9rg\_\_rpY8qb4Taa2BrqZjia-  
o54c\_BwmQUyDbkaK5zQ.docx  
CROSS\_FROM:  
CROSS\_MD5 HASH: 01CD48CE803BAEBF6828157CBF84713D  
CROSS\_MESSAGE ID:  
CROSS\_OWNER: rhalavati@google.com  
CROSS\_PRODVAL: CROSS-PROD002  
CROSS\_REDACTED: N  
CROSS\_SUBJECT:  
CROSS\_TITLE: 1- Incognito Mode Current and Possible Promises  
CROSS\_TO:  
CUSTODIAN/SOURCE: Helen Harris  
DATECREATED: 07/31/2018  
DATELASTMOD: 12/14/2018  
DATERCVD:  
DATESENT:  
DeDupedCustodians:  
DOEXT:  
FILENAME: 1- Incognito Mode Current and Possible\_1j9rg\_\_rpY8qb4Taa2BrqZjiao54c\_B-  
wmQUyDbkaK5zQ.docx  
ILS\_ProdDate: 05/07/2021  
CROSS\_ILS\_ProdDate: 09/01/2021  
MD5 HASH: 01CD48CE803BAEBF6828157CBF84713D  
MessageID:  
NATIVEFILE:  
Owner:  
PAGES:

REDACTED: N  
SUBJECT: